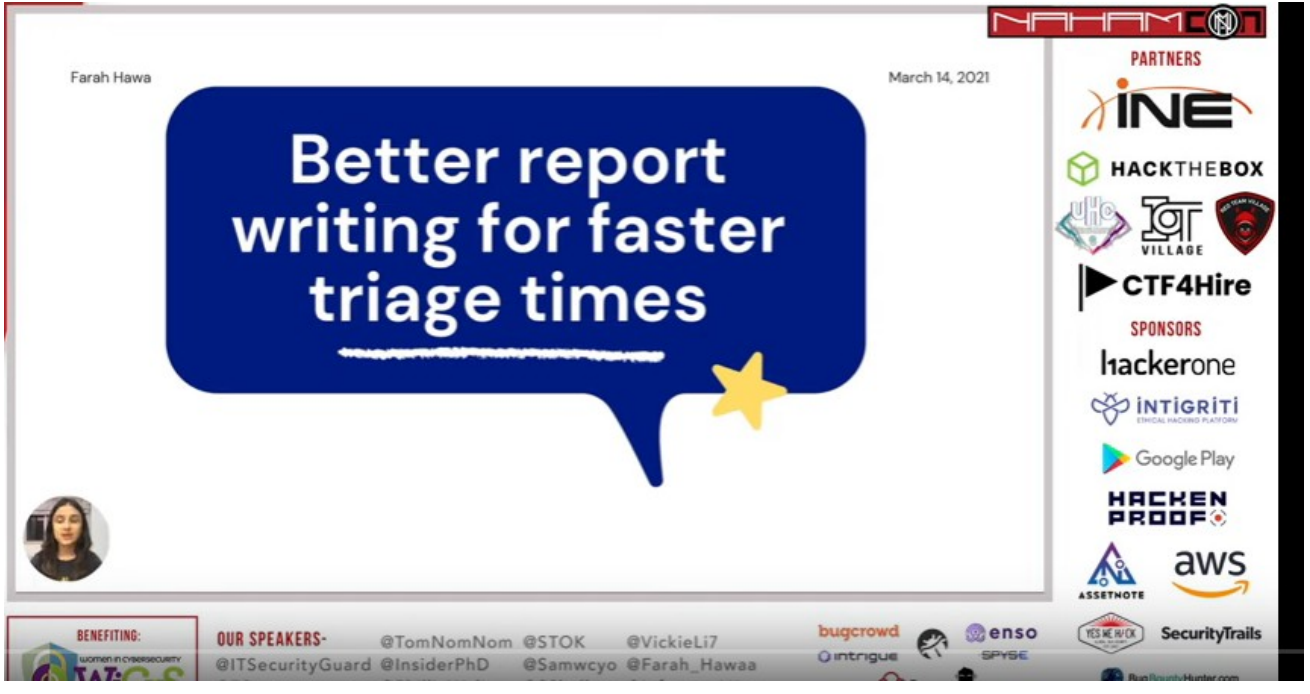
Infosec101

Reporte de resultados:
Fundamentos para escribir reportes efectivos

No reinventar la rueda

- Contenido basado en la ponencia “better report writing for faster triages times” por Farah Hawa durante Nahamcon 2021



1. Por qué un reporte

- Es el activo de mayor valor para el cliente puesto que contiene la evidencia de los hallazgos durante un pentesting o bug hunting
- En el reporte se encuentra los pasos para reproducir nuestros hallazgos y la evidencia del impacto de éstos

2. Características de un reporte inefectivo

- Comunicación inefectiva entre el investigador y la contraparte técnica del cliente
- Proceso ineficiente de reproducción de los hallazgos
- Falta de claridad en el impacto de los hallazgos
- Parrafos excesivamente largos
- Utilización de plantillas
- Inclusión de credenciales, cookies, tokens y otros elmentos técnicos que no son de utilidad en un documento

3. Presentar hallazgos de manera efectiva

- BUENA PRACTICA:
- 1. usar la siguiente dirección y validarse como atacante: https://www.micliente.com/perfil
- 2. Hace click en la pestaña “web”
- 3. Validarse como “victima”
- 4. Acceder a: https://www.micliente.com/comentar

- MALA PRACTICA:
- 1. Validarse como atacante, click en la pestaña “perfiles”, y luego buscar la pestaña “web”, hacer click en ésta
- 2. Desde una cuenta victima, ir a la sección de comentar y buscar el comentario que el atacante puso

4. Agregar una prueba de concepto (POC)

- Es la guía para reproducir cada hallazgo que se esta documentando:
- Puede incluir:
  - Un link que sea el resultado de una vulnerabilidad (por ejemplo un Cross Site Scripting (XSS)
  - Un archivo HTML producto de un request HTTP enviado como prueba para demostrar un Cross Site Request Forgery (CSRF)

5. Video para demostrar un POC

- Debe ser corto y si es necesario debe editarse hasta alcanzar una versión que comunique los resultados de manera efectiva
- No escribir pasos o comentarios en un block de notas durante el video
- Buena calidad del video en cuanto a resolución y audio
- Puede utilizarse musica sutil de fondo
- Subir el video a la plataforma vimeo protegido por password

6. Elementos que complementan el reporte

- Mencionar la vulnerabilidad(es) encontradas especificando nombres técnicos y una breve explicación o bien referencias bibliográficas / webgrafía
- Enfocarse en resaltar el impacto de los hallazgos
- Si se hace referencia a un video POC especificar marca de tiempo exacta
- Especificar si victima/victimario debe estar autenticado
- Capturas de pantalla pueden ayudar
- Incluir URLs relacionados a la vulnerabilidad (por ejemplo EndPoints)
- Si la vulnerabilidad requiere multiples roles especificar los pasos para cada uno de éstos

7. Demostrar impacto

- Pre-requisitos del atacante: víctima y aplicación
- En qué condiciones puede explotarse la vulnerabilidad? Qué perfil de usuarios pueden estar interesados en esta?
- Cómo afecta la vulnerabilidad las operaciones de la aplicación / usuarios?
- Presentar escenarios de ataques

8. Check list del reporte

- Escribir pasos cortos y claros en lugar de parrafos largos
- Incluir un POC
- Verificar las características del video(s) relacionados al POC
- Mencionar marca de tiempo del video cuando se haga referencia a éste
- Especificar los pasos/roles de las cuentas de usuarios involucradas
- Revisar al menos 2 veces hasta entregar el informe final

9. Check list para mostrar impacto

- Definir la posición inicial del atacante
- Definir posición inicial de victimas y otras presunciones
- Mencionar los pre-requisitos de la aplicación y del atacante

Referencias

- Youtube.com/c/FarahHawa
- @farah_hawaa
- https://www.bugcrowd.com/blog/writing-successful-bug-submissions-bug-bounty-hunter-methodology/