# I BUG BOUNTY IES ZAIDIN VERGELES

## Descripción de la tarea

Este concurso está dirigido al alumnado matriculado en el Curso de Especialización en Ciberseguridad en entornos de las Tecnologías de la Información y la Comunicación. El objetivo del mismo es fomentar el espíritu investigador y la ética hacker en el descubrimiento de vulnerabilidades.

El concurso se desarrollará entre el 21 de mayo y el 13 de junio con arreglo a las siguientes

**Bases**

*Primera. Inscripciones.*

1. El alumnado interesado en participar deberá informar de ello mediante correo electrónico al tutor del grupo.

2. La participación en el concurso supone la aceptación de las normas establecidas en estas bases.

*Segunda. Deber de confidencialidad.*

1. No se podrán hacer públicos los datos confidenciales a los que se haya podido acceder en el transcurso del concurso.

2. No se podrán publicar, por ningún medio, detalles de las vulnerabilidades encontradas en el plazo de 6 meses.

*Tercera. Reporte de vulnerabilidades.*

1. Todas las vulnerabilidades deberán reportarse en un único documento PDF que contendrá, para cada vulnerabilidad:

   a) Explicación de la vulnerabilidad y los pasos detallados para detectarla y explotarla.
   b) Acciones propuestas para mitigar o corregir la vulnerabilidad.
   c) Categoría en la que se clasifica la vulnerabilidad con arreglo a la tabla de la base *Quinta*.

2. El formato y estilo del documento deberá tener un acabado profesional, bien redactado, sin faltas de ortografía, uso de índices de contenido e índice de figuras, títulos de epígrafes, etc.

*Cuarta. Ámbito del concurso.*

1. El ámbito del concurso tendrá las características de una auditoría perimetral de caja negra.

2. Podrá ser objeto del test de intrusión cualquier servicio accesible desde Internet.

3. No se permiten los ataques de phishing ni el robo de credenciales por cualquier medio.

4. Los ataques de fuerza bruta sobre servicios o formularios de autenticación estarán limitados a horarios de poca productividad (horario no lectivo del centro) y siempre limitando el número de peticiones simultáneas que pueden realizarse y la duración en el tiempo a un máximo de 10 minutos y una sola vez

al día. En cualquier caso, estos ataques deberán estar debidamente justificados y fundamentados en el proceso de la auditoría.

*Quinta. Valoración del informe.*

El informe del test de intrusión será valorado por el equipo educativo y tendrá en cuenta la siguiente puntuación.

a) Calidad del informe: hasta 5 puntos.

b) Vulnerabilidades descubiertas. Se puntuarán con arreglo a la siguiente tabla.

| Categoría | Ejemplos | Puntos |
|---|---|---|
| Escalada de privilegios | Acceso a consolas de administración, administrador de dominio, pivoting en la red internet, etc. | 10 |
| Remote Code Execution. | Inyección de comandos, fallos de deserialización, etc. | 8 |
| Acceso no restringido al sistema de archivos o bases de datos. | SQLi, XXE, etc. | 6 |
| Security bypass. | Errores lógicos o bugs que permiten evitar restricciones de seguridad. | 5 |
| Ejecución de código en cliente. | XSS. | 4 |
| Otras vulnerabilidades menores | Fugas de información, configuración de seguridad poco adecuada, etc | 2 |

c) Vulnerabilidades encadenadas. Una misma vulnerabilidad puede encadenar vulnerabilidades de diferentes categorías que serán valoradas de forma individual siempre y cuando estén perfectamente explicadas y contempladas en el informe.

*Sexta. Premios.*

1. Los premios del concurso serán los siguientes.

a) Ganador: Libro de ciberseguridad + disco SSD

b) Segundo clasificado: Disco SSD

c) Tercer clasificado: Disco SSD

d) Resto de participantes: Reconocimiento