CIENCIA ABIERTA

JOSÉ L. BERENGUEL

UNIVERSIDAD DE GRANADA

DEPARTAMENTO DE Didáctica DE LAS Ciencias Experimentales

● Los alumnos de FP del Curso de Ciberseguridad se clasifican en el puesto 181 de un total de 8.130

FOTOS: C. A.

Foto de familia del equipo granadino del IES Zaidín Vergeles.

Del aula al podio: IES Zaidín-Vergeles en el Top 200

EL IES Zaidín-Vergeles de Granada ha participado con el alumnado de Formación Profesional matriculado en el Curso de Especialización en Ciberseguridad en Entornos TIC en una competición de *hacking*, el *Cyber Apocalypse*, organizado por la plataforma Hack The Box. El equipo llamado Zaid1nH4ck3rs ha quedado clasificado en la posición 181 de un total de 8.130 equipos de todo el mundo. La modalidad en la que se enmarca esta competición es conocida como *Capture The Flag* (CTF) o Captura la Bandera, ya que tras resolver el reto se descubre un secreto oculto llamado *flag* que reconoce a aquellos que lo encuentran los conocimientos y habilidades necesarias que se han utilizado para descubrirlo. El acceso a los cursos de especialización, también llamados Máster de FP, requiere que el alumnado haya cursado previamente un Ciclo de Formación Profesional de Grado Superior. Las competencias que el alumnado del Curso de Especialización en Ciberseguridad debe adquirir al finalizar su formación están recogidas en el Real Decreto 479/2020, entre ellas están detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados, y realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.

La participación en el *Cyber Apocalypse* fomenta que el alumnado adquiera estas y otras competencias a través del aprendizaje basado en retos (ABR), metodología en la que se desarrollan habilidades a través de la resolución de problemas reales. Para lograr el puesto 181, el alumnado tuvo que resolver 61 del total de 77 retos de los que estaba compuesto el concurso. Los retos se clasifican por categorías y dificultad. Las categorías presentes engloban tecnologías como *blockchain*, inteligencia artificial, *machine learning*, criptografía, programación segura, búsqueda de información en fuentes abiertas, análisis forense, *hacking web*, ingeniería inversa y explotación binaria. En cada uno de estas categorías existían retos de diferentes dificultades, entre muy fácil y difícil. Para resolver un reto es necesario analizarlo y estudiarlo para encontrar la vulnerabilidad o vulnerabilidades que están presentes en él. Por ejemplo, en los retos de criptografía es habitual analizar el código de un programa que cifra las comunicaciones. El código vulnerable habría sido escrito por algún programador poco experto que utiliza configuraciones inseguras de algoritmos de cifrado, lo que supone un riesgo para la privacidad de los mensajes que se han intercambiado. En la categoría de inteligencia artificial se trataba de obtener información secreta engañando o manipulando a una IA conversacional similar a ChatGPT, este ataque se conoce como *prompt injection*.

Julio Moreno del Ojo, alumno del curso, nos detalla uno de los retos resueltos en la categoría de hacking web. La web auditada presentaba un juego de fantasía en línea que, a simple vista, parecía un portal inofensivo para crear personajes, completar misiones y disfrutar de aventuras. Sin embargo, la forma en la que el juego manejaba los datos enviados por los jugadores presentaba un riesgo grave: en lugar de limitarse a modificar detalles inocentes como el nombre, la clase o la edad del personaje, el sistema permitía que la información externa interfiriera con configuraciones esenciales del servidor. El problema surge al "unir" sin controles adecuados los datos que cada usuario envía –por ejemplo, para cambiar su equipo o añadir una nueva habilidad– con la configuración interna de la aplicación. Esta vulnerabilidad, llamada *Prototype Pollution*, abre la puerta a que un atacante inserte "propiedades" o ajustes maliciosos que afectan al comportamiento del propio sistema. En otras palabras, el atacante no solo cambia su personaje, sino que consigue modificar partes del código que deberían ser intocables. Gracias a este agujero de seguridad, el servidor pasa a ejecutar órdenes externas –sin darse cuenta de que son maliciosas– y termina facilitando el robo de información privada o el control parcial de la infraestructura. En contextos reales, un fallo así permitiría vulnerar bases de datos, obtener información confidencial o incluso manipular servicios internos. Este reto pone en evidencia la importancia de validar toda la información que envían los usuarios a los servidores de Internet.

Certificado del ranking en la competición.

No todos los retos implican conocimientos técnicos en informática. Existen otros desafíos como la búsqueda de información en fuentes abiertas, conocida como OSINT (*Open Source Intelligence*), en donde se usan herramientas accesibles para cualquier persona. Nuestro alumno Pablo Sánchez Hidalgo explica cómo se resolvió un reto de este tipo en el que se presentaba una imagen donde se observaba una casa, un vehículo con la matrícula borrosa y algo de vegetación. Para resolver el reto había que localizar el nombre de la calle y la localidad donde se situaba la vivienda. A través del análisis de los elementos de la fotografía, como puede ser el tipo de vegetación, diseño de las casas y la matrícula del vehículo se pudo deducir en qué país fue tomada la imagen. A partir de ahí se realizó una investigación más detallada en aplicaciones de mapas para poder determinar con exactitud el Estado y la ciudad donde se había tomado la foto.

> Existen además otros desafíos como la búsqueda de información en fuentes abiertas

Las competiciones de ciberseguridad en general, y de hacking en particular, simulan casos reales de sistemas informáticos vulnerables que están conectados a Internet. La participación en ellas supone un beneficio para la formación del alumnado, ya que será la labor que realizarán en la vida real como profesionales dedicados a mejorar la seguridad de estos sistemas. Este es el cuarto año consecutivo que el alumnado matriculado en el Curso de Especialización en Ciberseguridad participa en el CTF *Cyber Apocalypse*. Cada año los resultados han ido mejorando, desde el puesto 1.818 de la edición de 2022, el 1.302 de 2023, la posición 412 en la edición de 2024 a este extraordinario Top 200 en 2025

▸**Sobre el autor:** José Luis Berenguel Gómez es doctor en Informática y profesor de Secundaria del IES Zaidín-Vergeles.