Señor
Adolfo Carlo Magno Castillo Meza
Jefe
Oficina Nacional de Procesos Electorales
Jr. Washington 1894
Lima

Asunto: Reporte de Vulnerabilidad Informática en Página Web de Hackathon 2018

De nuestra consideración:

Hiperderecho es una asociación civil peruana sin fines de lucro dedicada a investigar y promover el respeto de los derechos humanos en entornos digitales, conformada por abogados, comunicadores, y tecnólogos. Como parte de nuestro trabajo, estudiamos todas las iniciativas de política pública y programas gubernamentales que puedan impactar el ejercicio de derechos y libertades en estos ámbitos. Desde el 2017, tenemos una activa tarea de investigación en seguridad informática habiendo reportado exitosamente vulnerabilidades en INEI,[1] RENIEC,[2] y SUNEDU.[3]

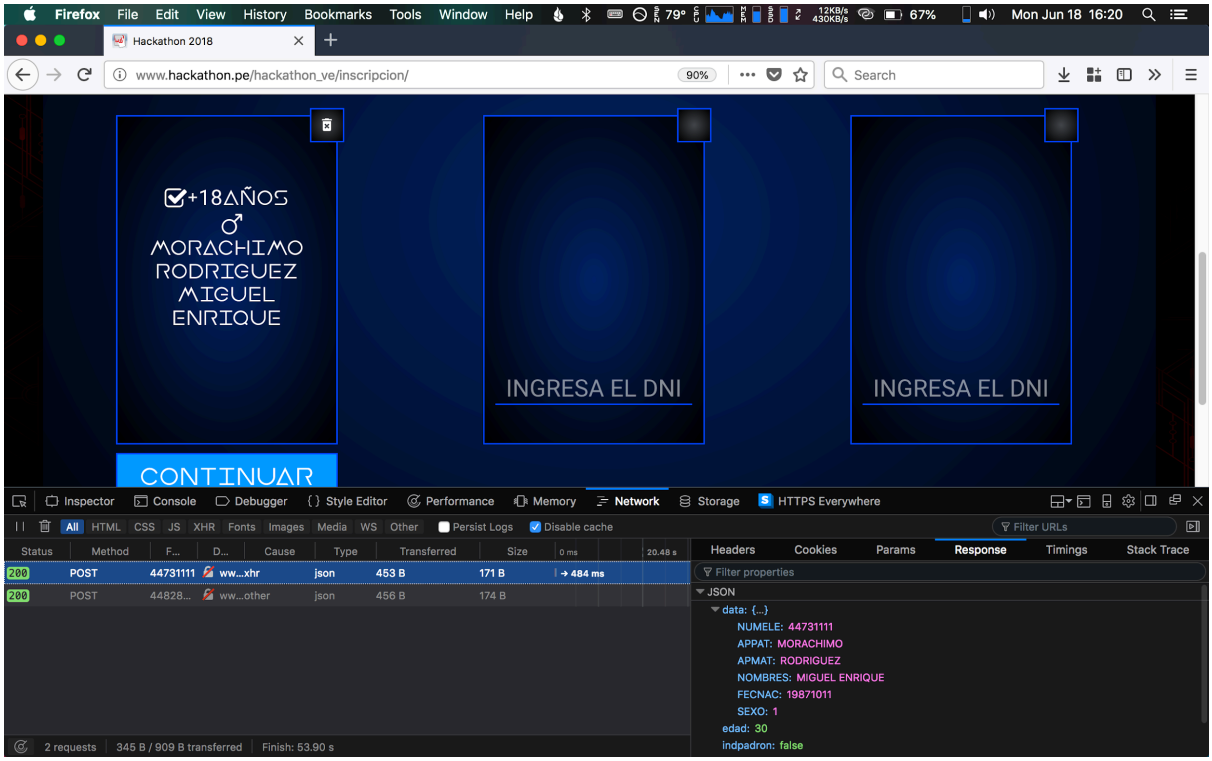
I. Vulnerabilidades detectadas

El motivo de nuestra carta es reportar oficialmente **dos (2) vulnerabilidades** en el sistema de registro de la Hackathon 2018 "Desafiando la Solución del Voto Electrónico Presencial," cuyo sitio web es http://www.hackathon.pe/. **Estas vulnerabilidades pueden ser explotadas por cualquier usuario sin necesidad de contraseñas, programas, o equipos especiales y ponen a disposición pública la información personal de los más de 23 millones de peruanos mayores de edad que conforman el padrón electoral.** Peor todavía, tenemos motivos para sospechar que una de estas vulnerabilidades está expuesta y explotable desde el año pasado en que se organizó la Hackathon anterior.

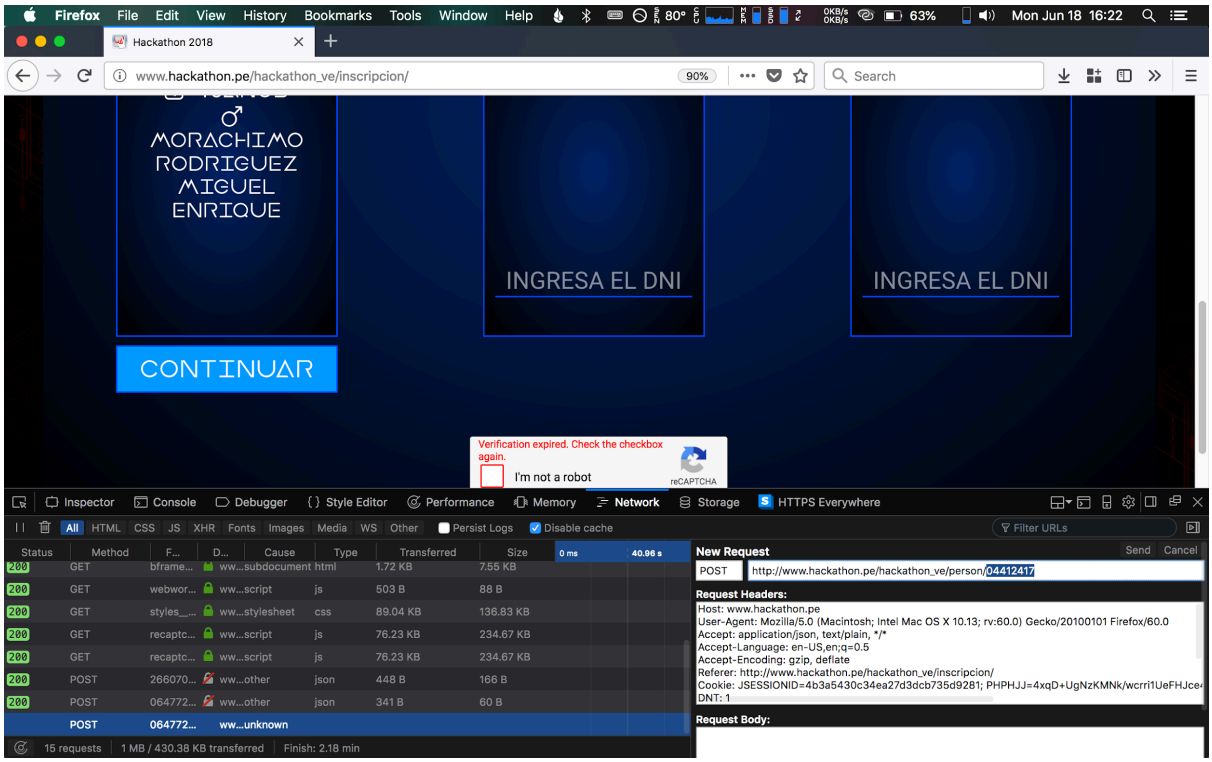
La **primera y más reciente vulnerabilidad** se encuentra en el actual formulario de inscripción de la Hackathon 2018 "Desafiando la Solución del Voto Electrónico Presencial" (www.hackathon.pe/hackathon_ve/inscripcion/). En esta página web, cuando se ingresa el dato Documento Nacional de Identidad en el campo para los miembros del equipo participante, el navegador hace una solicitud bajo el "método POST" a la dirección **http://www.hackathon.pe/hackathon_ve/person/[DNI]** donde [DNI] corresponde al número de DNI del participante.[4] Usando las Herramientas de Desarrollador disponibles en cualquier navegador de Internet es posible apreciar cómo el sistema de ONPE devuelve la información completa de nombres, edad, fecha de nacimiento, número de documento y sexo de la persona seleccionada consultando la misma dirección.

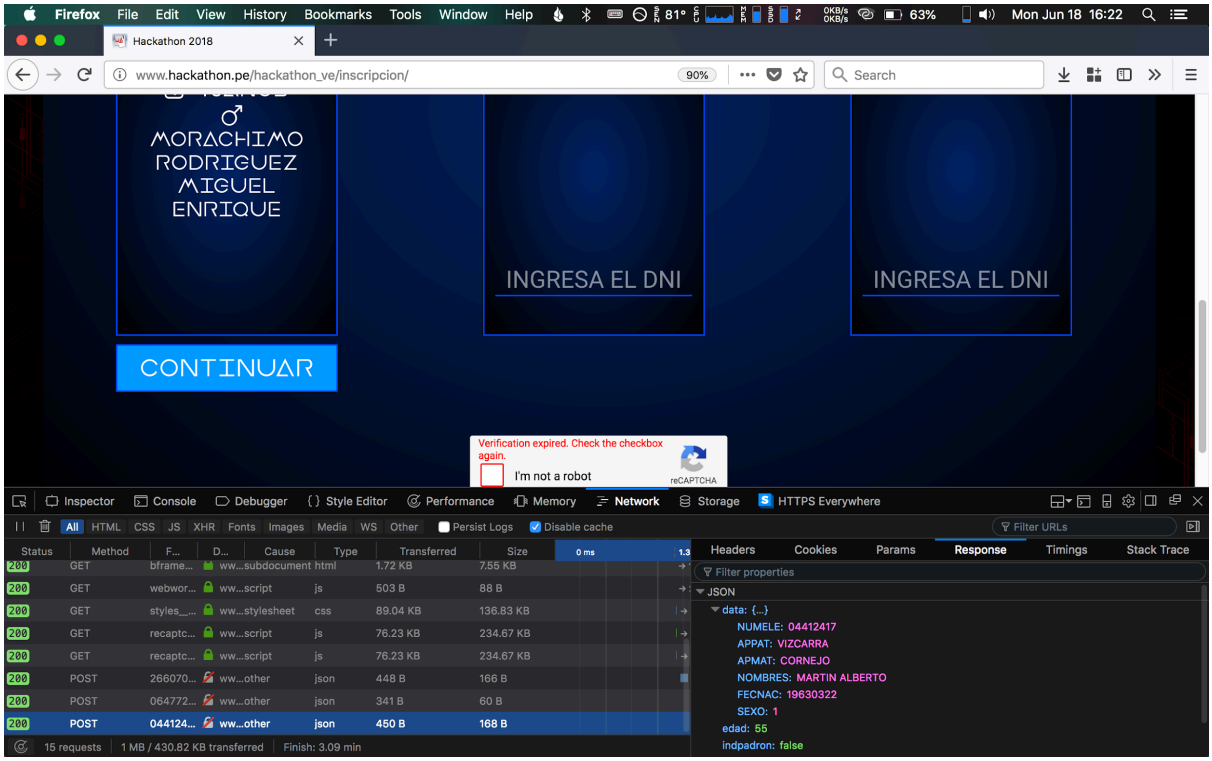
---

1 https://hiperderecho.org/2017/05/encuesta-lgbti-inei-fallo-seguridad-solucionado/
2 https://hiperderecho.org/2018/06/fallo-de-seguridad-permitia-descargar-la-foto-del-dni-de-todos-los-peruanos/
3 https://hiperderecho.org/2018/01/sunedu-datos-personales-filtrado/
4 Nuestra investigación ha documentado que entre el viernes 8 de junio, cuando se publicó originalmente el formulario, y la tarde del viernes 15 de junio el método de consulta no era POST sino GET. Esto significa que la información, además de ser accesible vía herramientas de desarrollador o la consola de comandos, también podía ser visualizado desde cualquier navegador web.



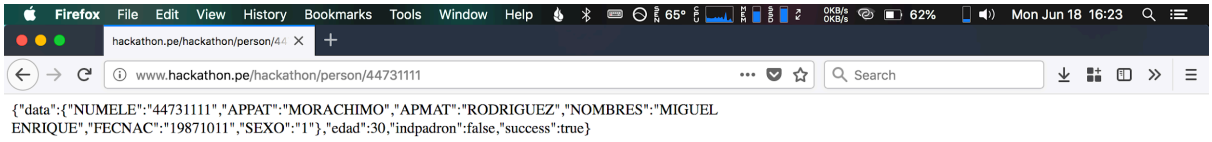
Por si no queda claro, esto significa que usando las mismas herramientas del navegador web es posible editar el pedido y obtener de la dirección web señalada la información de cualquier otra persona. La siguiente captura de pantalla muestra el pedido realizado sobre la información del Presidente de la República.





Esta información, además, por la forma en la que es entregada a través de esa dirección de Internet puede ser extraída de manera masiva aprovechando la secuencialidad de los números de DNI desde una consola de comandos o terminal usando métodos muy conocidos como “curl”. En el video contenido en el DVD que adjuntamos a esta carta se puede apreciar una prueba de concepto realizada por nuestro equipo de cómo podría explotarse esta vulnerabilidad, con gravísimas consecuencias para la privacidad de todos los peruanos (Anexo A).

La **segunda vulnerabilidad** fue descubierta a propósito de la primera. Según nuestra investigación, no es la primera vez que se organiza un evento de este tipo en su institución y no es la primera vez que se usa ese mismo formulario. Así, el formulario para la Hackathon 2017 era idéntico y se usó el mismo código fuente. En aquella ocasión, la información de los usuarios era consultada mediante un “método GET” a través de la ruta **http://www.hackathon.pe/hackathon/person/[DNI]** donde [DNI] corresponde al número de DNI del participante. Al igual que en el caso anterior, la solicitud entrega al usuario la información completa de la persona incluyendo nombres, edad, sexo, y número documento de identidad. A su vez, siguiendo el método arriba descrito, es posible editar la solicitud para obtener la información de otra persona. Adicionalmente, dado que se usa el método GET para obtener la información, es posible visualizar la respuesta en texto plano en la pantalla del mismo navegador. La existencia de una vulnerabilidad de este tipo que se desprende de un formulario que se usó hace más de un año nos hace pensar que es perfectamente posible que durante los últimos doce meses esta información haya estado accesible a cualquiera sin que su institución lo sepa.



Como puede apreciarse, ambas vulnerabilidades reportadas son muy graves porque exponen los datos de carácter personal de millones de peruanos a cualquier usuario de Internet. Esto no solo representa una trasgresión a la Constitución y sus normas de desarrollo, como la Ley de Protección de Datos Personales, sino que coloca en situación de riesgo físico y viola la privacidad de todos nosotros. De la misma manera, debilita la credibilidad de su institución como entidad capacitada para desplegar soluciones tecnológicas más complejas como las del voto electrónico presencial o la confidencialidad del proceso electoral.

II. Preguntas pendientes

Como investigadores en ciberseguridad, el motivo de nuestra carta es ponerlos sobre aviso de la existencia de estas vulnerabilidades. Nuestro procedimiento de divulgación responsable nos obliga primero a comunicarlo a quienes pueden solucionarlo y esperar durante un tiempo prudencial su respuesta antes de difundirlo públicamente. Por eso, al tiempo que recibe esta Carta, hemos enviado un reporte similar a la Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas de la Administración Pública del Perú (PeCERT). Estamos muy preocupados por este problema y esperamos que su institución pueda resolverlo en el más corto plazo.

Saludamos la iniciativa de su institución por promover un encuentro entre la comunidad de desarrolladores y un asunto de interés público como los próximos procesos electorales a través de una Hackathon. Creemos que esta relación no debe de solo agotarse en eventos de difusión sino que debe de ser una real conversación de ambos lados, respetando el legítimo interés que la sociedad civil, la prensa y ciudadanos informados puedan tener sobre el tema. Nuestra democracia no está construída sobre la buena fe de los funcionarios públicos sino sobre la transparencia y el equilibrio de poderes. Por ende, no se trata de confiar o no confiar en la capacidad de nuestras instituciones sino en la legitimidad que éstas construyen a través de la transparencia y la rendición de cuentas.

Por nuestro lado, no buscamos ninguna recompensa ni beneficio económico. Sin embargo, sí consideramos que sería muy transparente de su parte responder las siguientes interrogantes de pleno interés público directamente a nosotros o a través del medio que considere pertinente dentro de un plazo razonable:

1. ¿Tenía su institución conocimiento de estas vulnerabilidades? ¿Desde cuándo?
2. ¿Sabe si en los últimos doce (12) meses las rutas http://www.hackathon.pe/hackathon/person/[DNI] y http://www.hackathon.pe/hackathon_ve/person/[DNI] han sido explotadas en forma masiva? ¿Tiene forma de conocerlo?
3. ¿Por qué cambiaron de un método GET a un método POST en el formulario de la Hackathon 2018 el último viernes 15? ¿Consideran eso una solución apropiada?
4. ¿Cuál es el origen del banco de datos personales que quedó expuesto a través de esas rutas? ¿De qué institución se obtuvo? ¿Cuántos ciudadanos abarca?
5. ¿Existe en su institución un proceso de auditoría de software o control de calidad previo a producción?
6. ¿Han considerado publicar todo o parte del software que hace posible la Solución de Voto Electrónico Presencial como una medida de legitimidad alternativa o complementaria a la realización de una competencia limitada en tiempo, espacio y formato?

Solicitamos a su institución tenga a bien recibir nuestro reporte y tome acciones inmediatas al respecto, remediando la vulnerabilidad y respondiendo a nuestras preguntas. Del mismo modo, si es necesaria alguna precisión o mayores alcances nos ponemos a su disposición para cualquier consulta sobre este o futuros proyectos de su institución.

Sin otro particular, le expresamos nuestros mejores deseos y mayor consideración.

Atentamente,

Miguel Morachimo Rodríguez
Director Ejecutivo

Diego Escalante Urrelo
Director de Tecnología

Asociación Civil Hiperderecho
Av. Benavides 1180, oficina 602, Miraflores
RUC: 20551193099
miguel@hiperderecho.org

Anexo A: DVD conteniendo video de 2 minutos y 24 segundos en el que se aprecia la ubicación de la vulnerabilidad, cómo puede explotarse manualmente y cómo puede explotarse de manera automatizada a través de un script de prueba de concepto.