

# Examen de nivel

*“The Kulkan way”*

1. Menciona algún libro relacionado a la seguridad informática o... alguna variante que hayas leído? De ser así, ¿cuál es tu favorito y por qué?

Mi libro preferido de los que leí relacionados a seguridad es sin dudas “**The Web Application Hacker’s Handbook**” 2 edition de Dafydd Stuttard y Marcus Pinto aunque tengo que admitir que no lo terminé, llegué a 3/4 y lo dejé en stand by justo en el momento que hice el cambio de trabajo.

Es un libro increíblemente bien explicado, técnico, con gráficos, imágenes, notas de los autores y bloques de código que te permiten entender conceptos complejos de forma más sencilla, llevándote al mismo tiempo por todo el proceso de web application assessment de forma prolja y sistemática. Creo que es un libro buenísimo para tener a mano y de guía (lamentablemente no es de bolsillo y tampoco es cómodo para leer viajando ja).

2. ¿Te anotaste en algún CTF alguna vez? Si así fuera, ¿qué te pareció?

Sí, me anoté en varios con rendimientos MUY variados. El que más disfruté fue un CTF que organizó el ITBA de forma presencial antes del comienzo de la pandemia junto a todas las restricciones.

En ese momento estaba como un tren con offensive, trabajando en Deloitte y estudiando por mi cuenta y ese CTF estuvo buenísimo porque además de ser presencial, se armaron unos equipos improvisados buenísimos estando ahí, todos super concentrados, comiendo, riéndonos y aprendiendo.

Fue la mejor experiencia de CTF que tuve... después hice otros pero todos onlines y solo (más trabado, más aburrido y ya trabajando en algo que no tenía nada que ver).

3. Si tuvieras que elegir; ¿qué es lo que te gustaría aprender de manera más prioritaria o inmediata de seguridad informática? ¿Qué dejarías para después, y por qué?

Sinceramente web application (no porque haya hablado con Agus antes!) y en segunda instancia pentesting en infra. Empecé a estudiar de vuelta usando Hack The Box Academy, siguiendo el path the Bug Bounty Hunter y devuelta super motivado.

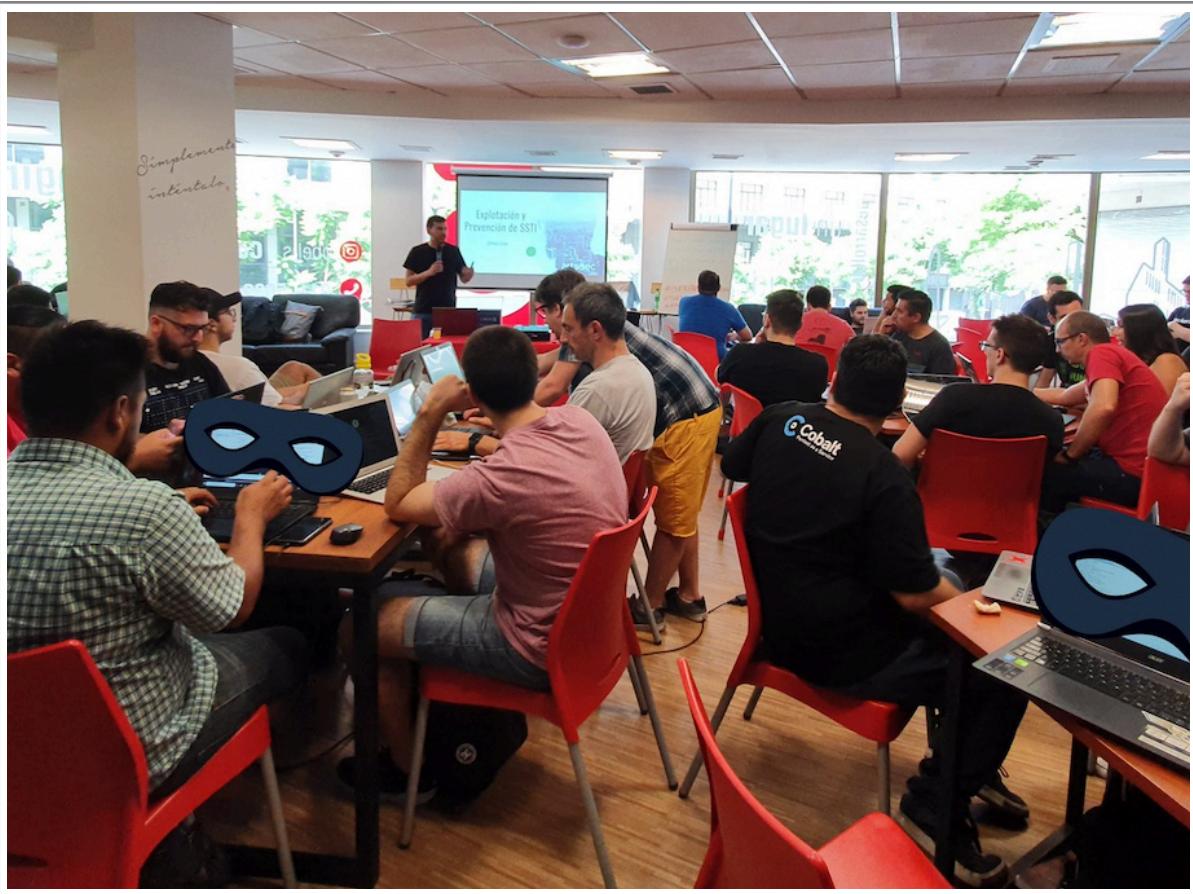
Dejaría para después toda la parte de gestión de la seguridad, todo lo que es armar inventarios de activos, planes de continuidad de negocio, planes de recuperación ante incidentes y todo eso... lo vi superficialmente cuando hice la Diplomatura en Seguridad Informática en la UTN (fue medio año armando una empresa ficticia para después hacer todos los cálculos y presentar los diferentes planes). Por ahora estoy seguro que es la rama que menos me interesa de nuestra área.

4. ¿Probaste participar de un Bug Bounty alguna vez? ¿Cómo fue tu experiencia?



Sí, participé del primer evento presencial del grupo Bug Bounty Argentina con HackerOne. Estuvo increíble, fue muy divertido y casi saqué una vulnerabilidad dentro del scope para Starbucks, quedé trabado. Básicamente había information disclosure en un path de Wordpress, con información del desarrollador y Web admin, además nombres aparentemente de usuarios... no me acuerdo muchos más detalles o de que

intenté hacer en su momento (fue antes de la pandemia también!). Pero bueno, justo fue un programa con presentaciones, regalos, sorteos, quizzes y hacking... no le faltó nada!



# Programando en Python

El código está en el repositorio privado compartido por mail.

# Redactando y comunicando

To: m.thanning@empresa.com  
Cc:  
Subject: Broken Access Control - IDOR  
From: Richie Prieto - richie.nprieto@gmail.com  
Message Size: 183 KB

Image Size: Medium

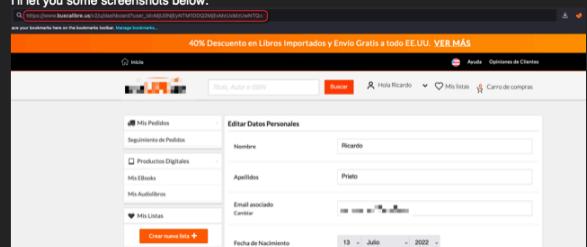
Hello Micaela, my name is Ricardo Prieto and I'm an Information Security professional and client of your company as well. I write to you directly because is the only email I found of your department. Basically, while using your site to buy a book, I came across with something unexpected. I found a vulnerability in your shopping web application that allows me to switch to other customer's carts by changing my user ID in the URL (I noticed it's base64 encoded).

The most critical thing about this, is actually that I was also able to access other clients private information by applying a exploiting a regular IDOR + decode/encoding. This make me very concern about all the private information that can be easily disclosed, so I'm really interested in help you and your tech team, to solve this issue as soon as possible.

Some information that I was able to access:

- First name
- Last name
- Address
- Email
- Cell phone number
- Latest purchases

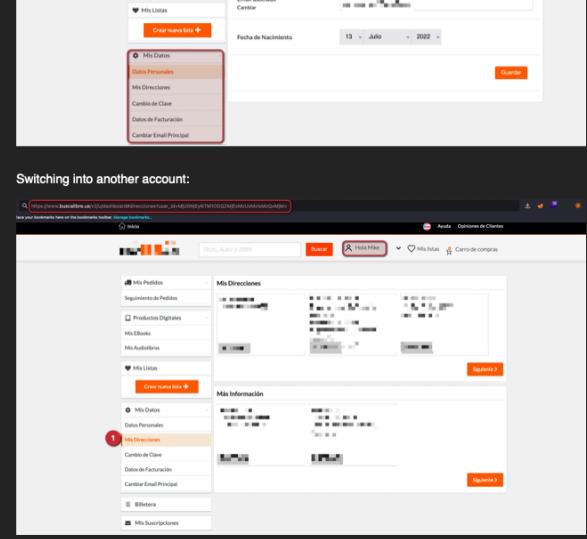
I'll let you some screenshots below:



To: m.thanning@empresa.com  
Cc:  
Subject: Broken Access Control - IDOR  
From: Richie Prieto - richie.nprieto@gmail.com  
Message Size: 183 KB

Image Size: Medium

Switching into another account:



IMHO I would suggest you change the HTTP method from GET to POST and would also try to avoid direct object references or at least improve the obfuscation mechanism (currently a regular Base64 encoding).  
Perhaps applying a salt value in a better hashing algorithm like SHA256 or SHA512 can improve the current state way more.

Micaela, please do not hesitate to contact me if you require further information, I will be happy to help you.  
Best,  
Ricardo Prieto

# El ojo crítico

Daniela está contenta. Es la primera vez en su vida que siente una sensación tan grande de satisfacción. "Lo logré, finalmente." - piensa. Hoy, Daniela se siente indestructible.

Daniela está contenta, es la primera vez en su vida que siente una sensación tan grande de satisfacción. «Lo logré, finalmente», piensa. Hoy Daniela, se siente indestructible.

---

De los nervios le tiembla levemente su mano izquierda, en la cual sostiene la entrada de cine Premium, para la cual esta vez no ha tenido que pagar dinero. La entrada posee un holograma con un código QR, el cual apunta a una URL que contiene la llave privada necesaria para verificar la firma digital.

De los nervios, le tiembla levemente su mano izquierda, en la cual sostiene la entrada del cine Premium (para la cual esta vez no ha tenido que pagar dinero). La entrada posee un holograma con un código QR, el cual apunta a una URL que contiene la llave pública necesaria para verificar la firma digital.

Acá me parece que está mal porque la llave privada es algo que solo debería conocer o tener ese usuario, una entrada de cine que te redireccione a una URL con una llave para verificar una firma digital... RARO (ni hablar que ya de por sí es raro que un cine tenga que ser firmado digitalmente).

En todo caso, debería tener la información de la llave pública para que al recibir la llave privada (que solo conoce ese usuario) se pueda concretar la firma digital.

---

"Tantas horas intentando explotar el blind SQL injection. Yo sabía que era explotable. Me río de tod@s aquell@s que abucheaban las excepciones del motor de SQL que compartía en los foros de Hacking." - piensa Daniela.

«Tantas horas intentando explotar el blind SQL injection, yo sabía que era explotable... me río de todos aquellos que abucheaban las excepciones del motor de SQL que compartí en los foros de Hacking.», pensó Daniela.

---

Para este caso estuve buscando porque pensaba que no había relación entre una blind injection y las exceptions de un motor de base de datos. Al parecer sí, incluso Burp Academy tiene un lab que creo que esta relacionado... obviamente lo vi por arriba nada más. Igualmente no estoy 100% seguro.

<https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors>

---

A mediados del año anterior, Daniela había invertido una insuperable cantidad de horas en descifrar el algoritmo utilizado en la carga de saldo de la SUBE. La aplicación de carga se comunicaba utilizando el protocolo HTTPS, por lo que Daniela pudo interceptar su tráfico de datos fácilmente al encender Certificate Pinning. En todo momento, Daniela estuvo a un par de bytes de realizar una carga clandestina satisfactoria (le faltaba exactamente escribir el valor 0x2P en el bit #4 del byte que estaba modificando), pero eventualmente la frustración ganó, y se dio por vencida.

A mediados del año pasado, Daniela había invertido una insuperable cantidad de horas descifrando el algoritmo utilizado en la carga de saldo de la SUBE. La aplicación de carga se comunicaba utilizando el protocolo HTTPS, por lo que Daniela pudo interceptar su tráfico de datos fácilmente al encender Certificate Pinning.

En todo momento, Daniela estuvo a un par de bytes de realizar una carga clandestina satisfactoria (le faltaba exactamente escribir el valor 0x2P en el bit #4 del byte que estaba modificando), pero eventualmente la frustración ganó, y se dio por vencida.

---

En este ejemplo, “encender Certificate Pinning” en realidad sería un intento de fortalecer aún más el protocolo SSL con un HTTP header deprecado.... haciendo que la aplicación solo acepte una o una serie de llaves públicas válidas, haciendo que el application web server de error al notar otra llave pública o conjunto de llaves públicas.

Y de binarios ya ahí... se me estalla la cabeza

---

Meses después de su fallido intento por viajar gratis en Subte, Daniela conoce a Gretta. Se enamora casi de inmediato; es mutuo. Gretta frecuentaba los mismos foros de Hacking que Daniela, y su relación había surgido producto de una discusión acerca de como desencriptar un Hash SHA-256. La discusión empezó siendo pública, y luego pasó a privada. Los mensajes entre Daniela y Gretta escondían algunas notas de amor, y los payloads que intentaban que la otra ejecute mutaron a ser cartas de presentación.

Meses después de su fallido intento por viajar gratis en Subte, Daniela conoce a Gretta. Se enamoró casi de inmediato; fue mutuo. Gretta frecuentaba los mismos foros de Hacking que Daniela, y su relación había surgido producto de una discusión acerca de cómo desencriptar un Hash SHA-256. La discusión empezó siendo pública, y luego pasó a ser privada. Los mensajes entre Daniela y Gretta escondían algunas notas de amor, y los payloads que intentaban que la otra ejecute mutaron a cartas de presentación.

---

En este ejemplo, el hashing no es un mecanismo de cifrado, por lo tanto no se pueden desencriptar para volver a tener su valor (nunca vamos a llegar a la fuente de la información, porque son funciones unidireccionales, X puede llegar a Y pero no Y a X).

---

Un viernes de lluvia quedaron en encontrarse, esta vez en persona, en un lugar de común acuerdo dentro del Shopping Abasto a las 13 horas y 37 minutos. Su encuentro dio inicio a una intensa relación. Programaban, debuggeaban y reverseaban juntas. Si una decía UDP SYN, la otra decía UDP ACK. Si una pensaba un puerto TCP entre 65000 y 80000, la otra adivinaba inmediatamente el número correcto. Pero lo que rápido comenzó, abruptamente terminó. Greta perdió interés, y dejaron de verse.

Quedaron en encontrarse un viernes de lluvia, esta vez, en persona y en un lugar de común acuerdo dentro del Shopping Abasto a las 13 horas y 37 minutos. Su encuentro dio inicio a una intensa relación, programaban, debuggeaban y reverseaban juntas. Si una decía UDP SYN, la otra decía UDP ACK, si una pensaba un puerto TCP entre 65000 y 80000, la otra adivinaba inmediatamente el número correcto. Pero lo que rápidamente comenzó, abruptamente terminó, Greta perdió interés, y dejaron de verse.

---

Se confundieron de protocolo, TCP funciona con paquetes SYN y ACK, UDP solo con request y response. Además, se excedieron un poco con los puertos, la cantidad total es 65535 puertos.

---

Daniela quedó destruida. Fue la intensidad de sus emociones canalizadas en el Hacking que progresivamente la llevaron a reencontrarse con esa necesidad de auto superación; con esa necesidad de “ser sudo en su propia vida”.

Daniela quedó destruida. Fue la intensidad de sus emociones, canalizadas en el Hacking, que progresivamente la llevaron a reencontrarse con esa necesidad de autosuperación... con esa necesidad de “ser sudo en su propia vida”.

---

Hoy, el boleto que Daniela sostiene en su mano derecha no solo representa un nuevo nivel de entendimiento técnico de SQL en su carrera profesional; sino que también implica tanto la posibilidad de sentirse superior a Greta, como la de poder volver a captar su atención.

Hoy, el boleto que Daniela sostiene en su mano derecha, no solo representa un nuevo nivel de entendimiento técnico de SQL en su carrera profesional; sino que también implica tanto la posibilidad de sentirse superior a Greta, como la de poder volver a captar nuevamente su atención.

---

El orgullo que siente por su logro, sumado a la necesidad de cerrar el circuito completo en su estructurada mente, la llevan a sentarse en la Butaca e intentar disfrutar de la película “Tortugas Ninja 2”, cuyo identificador de Row desafortunadamente estaba primera en la tabla de películas sobre la cual tomó parcial control mediante JavaScript. El respaldo del asiento ubicado delante del suyo muestra un garabato escrito en graffiti, “RFCREB DHR NYTHA QVN CHRQNF CREQBANEZR”. Daniela lo mira y ríe – “Parece que al cine vienen extraterrestres” – piensa.

El orgullo que siente por su logro, sumado a la necesidad de cerrar el circuito completo en su estructurada mente, la llevan a sentarse en la butaca e intentar disfrutar de la película “Tortugas Ninja 2”, cuyo identificador de Row desafortunadamente estaba primero en la tabla de películas sobre la cual tomó parcial control mediante JavaScript. El respaldo del asiento ubicado delante del suyo muestra un garabato escrito en graffiti, “RFCREB DHR NYTHA QVN CHRQNF CREQBANEZR”. Daniela lo mira y ríe – “Parece que al cine vienen extraterrestres” – piensa.

---

Como costó este... ESPERO QUE ALGUN DIA PUEDAS PERDONARME es el verdadero mensaje oculto en el graffiti. Claramente Daniela mal interpretó el mensaje que estaba cifrado usando ROT13.

---

Finalizados los anuncios, la sala de cine reduce la intensidad de la luz en los pasillos, y aumenta el volumen de efectos de sonido, preparando a l@s presentes para disfrutar de una experiencia única en un mundo donde las tortugas comen pizza y saben artes marciales. Daniela, quizás en un acto de premonición, estira los brazos y se despereza. Repentinamente, un frío metálico abraza su muñeca izquierda. Acto seguido, escucha el susurro de una persona cuya voz le resulta muy familiar. - “Daniela Gonzalez, queda usted detenida por fraude informático.”

Finalizados los anuncios, la sala de cine reduce la intensidad de la luz en los pasillos y aumenta el volumen de efectos de sonido... preparando a los presentes para disfrutar de una experiencia única, en un mundo donde las tortugas comen pizza y saben artes marciales. Daniela, quizás en un acto de premonición, estira los brazos y se despereza. Repentinamente, un frío metálico abraza su muñeca izquierda; acto seguido, escucha el susurro de una persona cuya voz le resulta muy familiar. - “Daniela Gonzalez, queda usted detenida por fraude informático.”

---

Nooo que giro inesperado de la historia. Moraleja, si querés probarte técnicamente mejor que sea en un ámbito legal, cobrá tu remuneración y pagá la entrada. No confies en Grettas, nunca.

---