o 18app utilizzando la propria identità digitale (SPID) per l’autenticazione dei richiedenti. Una volta acceduto al sistema Luca ha cominciato a studiare il sito web, concentrandosi sulla procedura per la richiesta del bonus, che consente di “partizionare” i 500 euro per spenderli nei vari servizi previsti. Luca ha creato un buono da 50 euro per studiare le richieste generate dal sistema come evidenziato di seguito.

La richiesta utilizza un formato JSON per contenere una serie di informazioni utili ad espletare la procedura. Per i non addetti ai lavori, immaginate il formato JSON come un contenitore che si compone dei seguenti parametri:

* idBeneficiario: l’ID del “mio” account;
* annoRif: l’anno in cui è stata spedita la richiesta (il [**Bonus Cultura**](http://www.techeconomy.it/tag/bonus-cultura/) è spendibile fino al 2018);
* idAmbito: la categoria del servizio (cinema, concerti, libri ecc…);
* idBene: la sotto-categoria del servizio (nel caso dei libri: audiolibro, ebook o cartaceo);
* importoRichiesto: l’importo da assegnare al buono.

Ricevuta la richiesta, il server fornisce una risposta con relativo esito. La risposta include ovviamente l’esito, i dati del richiedente, identificativo del buono, e molto altre informazioni private. Ed ora iniziano le note dolenti!

Luca scopre che **manipolando il parametro idBeneficiario è possibile creare buoni utilizzando un account altrui**. Inoltre, dalla risposta è possibile **ottenere le informazioni dell’account legittimo che di cui abbiamo usato l’ idBeneficiario con conseguente data leak**.

Altra vulnerabilità riscontrata è una **falla “Broken Access Control” che è presente nella richiesta di all’annullamento** dei buoni creati.

“*La richiesta GET in questione si trova nel seguente formato: https://www.18app.italia.it/BONUSWS/rest/secured/gestioneVoucher/annullaVoucherOnline/****ID.****L’ID del buono evidenziato sopra è ottenibile tranquillamente leggendo la risposta della generazione del voucher. La falla risiede nella possibilità di modificare tale parametro, che potrebbe portare a risultati disastrosi per il portale, quale appunto****la cancellazione di tutti i buoni di tutti gli utenti****.*” Spiega Luca Milano [**nell’analisi che ha pubblicato sul suo blog**](https://lmilano.blogspot.it/2016/11/come-violare-18app-per-avere-il-bonus.html).

E non finisce qui. Luca trova altre falle relative a richieste che permettono di trovare informazioni sensibili (anagrafica, disponibilità del bonus ecc..) di altri utenti registrati, semplicemente avendo il loro codice fiscale (CF).

Le richieste sono:

* https://www.18app.italia.it/BONUSWS/rest/secured/18enne/beneficiario/**CF**
* https://www.18app.italia.it/BONUSWS/rest/secured/18enne/listaVoucherDaSpendere/**CF**
* https://www.18app.italia.it/BONUSWS/rest/secured/18enne/borsellino/**CF**

*“Le vulnerabilità appena documentate pongono la piattaforma ad un livello di rischio relativamente alto dato che un malintenzionato potrebbe impossessarsi dell’intero bugdet assegnato al Bonus Cultura (ovviamente quello non ancora usufruito) semplicemente combinando le richieste appena trattate.”*Spiega Luca.

Le scoperte di Luca risalgono al 14 novembre scorso quando, con il supporto dell’esperto [**Paolo Stagno**](http://paolostagno.com/), fondatore del progetto italiano **[VoidSec](https://voidsec.com/)**, ha deciso di **riportare le falle in maniera etica al CERT Nazionale e SOGEI**, la società che gestisce il sistema informativo del MEF e che ha curato la pubblicazione del sito 18app.italia.it.