

APPLICATION ANALYSIS

A cura di:

Luca Pezzolla 0124/002411

Fulvio Serao 0124/002423

0124/002423 0124/002423



INTRODUZIONE

Il nostro lavoro di application analysis vede coinvolte diverse applicazioni target, al fine di evidenziarne eventuali criticità dal punto di vista della sicurezza. Vista la loro capillare diffusione negli ultimi anni, è stato posto l'accento su:

- **Vinted**
- **Wallapop**
- **Subito**

Che rappresentano un esempio perfetto del mercato dell'usato in Italia.

A tal proposito gli strumenti scelti per raggiungere i nostri obiettivi sono stati Charles Proxy e Burp Suite.

Charles Proxy è uno strumento di debugging HTTP che consente la visualizzazione del traffico HTTP e SSL/HTTPS tra la propria macchina e Internet.

Burp Suite è uno strumento che include un insieme di tools per testare la sicurezza delle applicazioni e ricercarne delle vulnerabilità.



PREMESSA

Per una più chiara comprensione del lavoro svolto nell'analisi delle applicazioni menzionate in precedenza, è necessario premettere che l'utilizzo di strumenti come Charles Proxy o Burp Suite è possibile solamente nel caso in cui il dispositivo che si sta utilizzando consenta la configurazione e l'utilizzo di un **Proxy**. La nostra analisi si concentra sul traffico HTTP e SSL/HTTPS che passa tra noi (*client*) e i *server* delle applicazioni che stiamo utilizzando. Ciò significa che ogni operazione che verrà mostrata da qui in poi è stata semplicemente effettuata utilizzando l'app/sito corrispettiva, per poi osservarne i risultati tramite Proxy.

Vinted

Vinted è un sito di vendita online con sede in Lituania per l'acquisto, la vendita e lo scambio di articoli nuovi o di seconda mano, principalmente abbigliamento e accessori.

Dei 30 milioni di membri dichiarati, 12 milioni sono in Francia.

Economicamente, Vinted è diventata una startup valutata oltre un miliardo di dollari.

Nel nostro paese l'utilizzo di Vinted ha avuto una grossa diffusione solamente negli ultimi anni. Lo slogan con il quale si è presentato a noi è stato "Non lo metti? Mettilo in vendita!". Qual è il livello di sicurezza fornito da Vinted?

AUTENTICAZIONE

Il primo aspetto analizzato è stato quello relativo all'autenticazione. In particolar modo, abbiamo cercato di capire se utilizzando Charles Proxy al momento dell'autenticazione su Vinted fosse possibile visualizzare le credenziali appena inserite. Vinted fornisce tre metodi di accesso: quello attraverso il proprio account Facebook, tramite l'account Google oppure mediante la più classica combinazione email/username e password.



```
{
  "client_id": "web",
  "scope": "user",
  "fingerprint": "a6e9c70ffd95d2841ea5aaalc0a6f69b",
  "username": "XXXXXXXXXXXXXXXXXXXX",
  "password": "XXXXXXXXXX",
  "uuid": "dbac6abc-d839-464a-9939-3e6b7ce41136",
  "grant_type": "password"
}
```

Informazioni visualizzate una volta effettuato l'accesso con username e password

```
{
  "client_id": "web",
  "scope": "user",
  "provider": "google",
  "assertion": "eyJhbGciOiJSUzI1NiIsImtpZCI6IjcxM2ZkNjhjOTY2ZTI5",
  "fingerprint": "a6e9c70ffd95d2841ea5aaalc0a6f69b",
  "grant_type": "assertion"
}
```

Informazioni visualizzate una volta effettuato l'accesso con un account Google

```
{
  "client_id": "web",
  "scope": "user",
  "provider": "facebook",
  "assertion": "EAAHItgsjHIsBAG6HYZBqniSU65FuZAnEZCQVP3r5Z",
  "fingerprint": "f5ac8000997dc97c76460765d2b74c38",
  "grant_type": "assertion"
}
```

Informazioni visualizzate una volta effettuato l'accesso con un account Facebook

Qualora l'utente si registrasse alla piattaforma tramite Google/Facebook, al momento dell'accesso saranno visibili soltanto le informazioni sulla fingerprint e sulla assertion; al contrario, le credenziali di accesso saranno visibili all'interno della **POST** che viene inviata a Vinted.

COSA POSSO VEDERE DEGLI ALTRI?

Le informazioni che **Vinted** salva dei suoi fruitori sono molteplici. Ci siamo quindi chiesti quali informazioni sensibili legate agli altri utenti potessimo vedere. Per dati sensibili, in questo contesto, si intende tutto ciò che non sarebbe possibile vedere con un normale utilizzo dell'app/sito web.



```
{
  "user": {
    "id": 58224596,
    "anon_id": "224613db-3746-4a1a-a66e-bddead45ae8",
    "login": "lucapezzolla",
    "real_name": null,
    "email": null,
    "birthday": null,
    "gender": "M",
    "item_count": 2,
    "msg_template_count": 4,
    "given_item_count": 4,
    "taken_item_count": 16,
    "favourite_topic_count": 0,
    "forum_msg_count": 0,
    "forum_topic_count": 0,
    "followers_count": 6,
    "following_count": 8,
    "following_brands_count": 5,
    "positive_feedback_count": 16,
    "neutral_feedback_count": 0,
    "negative_feedback_count": 0,
    "meeting_transaction_count": 0,
    "account_status": 0,
    "email_bounces": null,
    "feedback_reputation": 1.0,
    "account_ban_date": null,
    "is_account_ban_permanent": null,
    "is_forum_ban_permanent": null,
    "is_on_holiday": false,
    "is_publish_photos_agreed": false,
    "expose_location": false,
    "third_party_tracking": true,
    "default_address": null,
    "created_at": "2021-04-10T12:48:20+02:00",
    "last_logged_on_ts": "2022-11-19T11:57:52+01:00",
    "city_id": 168898,
    "city": "",
    "country_id": 18,
    "country_code": "IT",
    "country_iso_code": "IT",
    "country_title_local": "Italia",
    "country_title": "Italia",
    "contacts_permission": null,
    "contacts": null,
  }
}
```

Le prime informazioni sensibili messe a disposizione da Vinted grazie a Charles Proxy riguardano una generale configurazione del profilo dell'utente su cui si sta "indagando". Tra le diverse cose, è possibile conoscere con precisione l'ultimo accesso e la data di creazione dell'account; inoltre, è possibile sapere se quest'ultimo sia stato bannato o meno permanentemente e se abbia dato il consenso al tracking di terze parti.

```
"donation_configuration": null,  
"fundraiser": null,  
"business": false,  
"business_account": null,  
"has_ship_fast_badge": false,  
"total_items_count": 6,  
"about": "",  
"verification": {  
  "email": {  
    "valid": true,  
    "available": true  
  },  
  "facebook": {  
    "valid": true,  
    "verified_at": "2021-04-10T12:48:12+02:00",  
    "available": true  
  },  
  "google": {  
    "valid": false,  
    "verified_at": null,  
    "available": true  
  },  
  "phone": {  
    "valid": true,  
    "verified_at": "2021-07-28T19:12:31+02:00",  
    "available": true  
  }  
}
```

Proseguendo con la ricerca, veniamo a conoscenza dei profili collegati all'account dell'utente. In questo caso sappiamo in che data l'utente ha verificato la sua email, il suo profilo Facebook e il suo numero di cellulare.

```
"closet_promoted_until": null,
"avg_response_time": null,
"carrier_ids": [59, 62, 67, 68, 100, 9, 10],
"carriers_without_custom_ids": [59, 62, 67, 68, 100],
"locale": "it-fr",
"updated_on": 1668355272,
"is_hated": false,
"hates_you": false,
"is_favourite": true,
"profile_url": "https://www.vinted.it/member/58224596-lucapezzolla",
"share_profile_url": "https://www.vinted.it/member/58224596-lucapezzolla",
"facebook_user_id": null,
"is_online": false,
"has_promoted_closet": false,
"can_view_profile": true,
"can_bundle": true,
"last_logged_on": "oggi 11:57 AM",
"location_description": null,
"accepted_pay_in_methods": [{
  "id": 1,
  "code": "CREDIT_CARD",
  "requires_credit_card": true,
  "event_tracking_code": "cc",
  "icon": "credit-card",
  "enabled": true,
  "translated_name": "Carta di credito/debito",
  "note": "Le tue informazioni per il pagamento non saranno mai condivise con chi vende e Vinted
}, {
  "id": 17,
  "code": "GOOGLE_PAY",
  "requires_credit_card": false,
  "event_tracking_code": "google_pay",
  "icon": "google-pay",
  "enabled": true,
  "translated_name": "Google Pay",
  "note": ""
}, {
  "id": 16,
  "code": "APPLE_PAY",
  "requires_credit_card": false,
  "event_tracking_code": "apple_pay",
  "icon": "apple-pay",
  "enabled": true,
  "translated_name": "Apple Pay",
  "note": ""
```

Di ogni utente è possibile sapere quali metodi di pagamento, tra quelli messi a disposizione da Vinted, sono stati attivati. In questo caso l'utente ha collegato al suo account una carta di credito, piuttosto che un account Google Pay o Apple Pay.

```
"business": true,  
"business_account": {  
  "id": [REDACTED],  
  "name": [REDACTED],  
  "legal_code": "889 [REDACTED]",  
  "email": "[REDACTED]@gmail.com",  
  "phone_number": "+33 [REDACTED]",  
  "legal_name": [REDACTED],  
  "nationality": "FR",  
  "vat": null,  
  "entity_type": "sole_trader",  
  "status": "completed",  
  "country": "FR",  
  "nationality_title": "Francia",  
  "country_title": "Francia",  
  "entity_type_title": "Ditta individuale"  
},
```

*Non possono dirsi al sicuro neppure i dati dei cosiddetti account **Business** iscritti alla piattaforma. Cercando, infatti, uno di questi profili su Vinted, tramite Charles Proxy siamo riusciti a trovare il numero di telefono collegato all'account. Le informazioni sensibili in questo caso erano molteplici (legal code, email) ma queste erano già visibili in chiaro sul profilo dell'utente in questione, fatta eccezione per il suo numero di telefono, non reperibile in nessun altro modo. Tutte queste informazioni sono state ovviamente oscurate per questione di privacy.*

COSA POSSO VEDERE DEL MIO ACCOUNT?

Successivamente ci siamo chiesti quali informazioni sensibili, relative all'account con il quale si effettua l'accesso, fossero visibili. In aggiunta a quanto mostrato in precedenza, riguardo i profili degli altri utenti, è stato possibile visualizzare dati ancora più delicati.



```
{
  "credit_card": {
    "id": 94729924,
    "user_id": 117907244,
    "user_address_id": null,
    "name": "Fulvio Serao",
    "brand": "MasterCard",
    "last_four": "XXXX",
    "external_code": 94729924,
    "expiration_year": "XXXX",
    "expiration_month": "XX",
    "is_default": true,
    "single_use": false,
    "expired": false
  },
  "authentication_redirect_url": null,
  "authentication_action": null,
  "code": 0
}
```

Tra le informazioni disponibili, è possibile vedere quelle relative al proprio metodo di pagamento collegato. Per la precisione è stato possibile vedere, in questo caso, le ultime quattro cifre della carta di credito, nome e cognome del titolare, l'anno ed il mese di scadenza.

```
{
  "bank_accounts": [{
    "id": [REDACTED],
    "name": "Luca Pezzolla",
    "account_number": [REDACTED],
    "routing_number": [REDACTED],
    "spending_type": null,
    "is_default": true,
    "user_id": 58224596,
    "user_address_id": 54671215
  }],
  "code": 0
}
```

Come se non bastasse, non è possibile vedere solo la carta di credito collegata all'account ma anche il proprio IBAN, seppur non per intero.

MESSAGGISTICA

Vinted mette a disposizione una chat tra gli utenti in modo tale che questi possano chiedere informazioni ulteriori relativamente ad un prodotto in vendita a cui sono interessati oppure fare un'offerta diversa rispetto al prezzo di partenza.

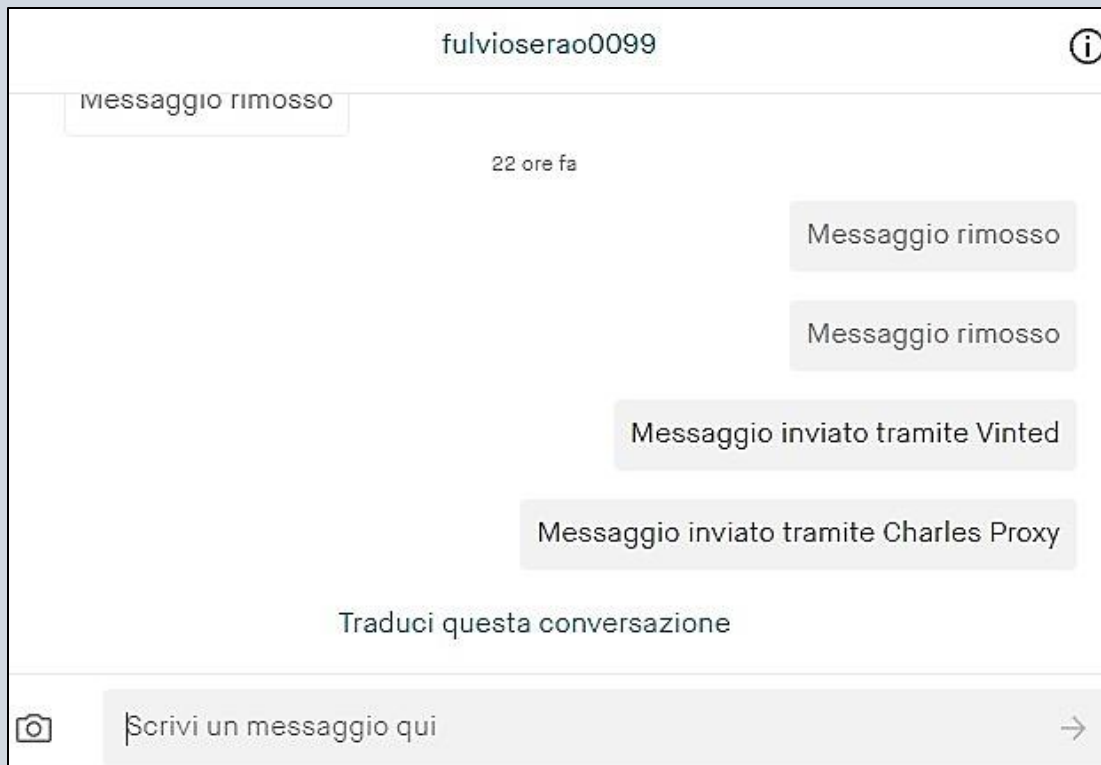


```
"conversation": {
  "id": 6187290644,
  "read_by_current_user": true,
  "read_by_opposite_user": false,
  "localization": "manual",
  "translated": false,
  "allow_reply": true,
  "is_suspicious": false,
  "subtitle": "questa e' una prova",
  "messages": [{
    "entity_type": "message",
    "entity": {
      "body": "Ared",
      "photos": [],
      "user_id": 117907244,
      "sent_via_mobile": true,
      "id": 16902687815,
      "reaction": null,
      "is_hidden": false
    },
    "created_at_ts": "2022-11-13T17:01:21+01:00",
    "created_time_ago": "13/11/2022"
  }, {
    "entity_type": "message",
    "entity": {
      "body": "Ciao Flavio",
      "photos": [],
      "user_id": 58224596,
      "sent_via_mobile": true,
      "id": 16902692985,
      "reaction": null,
      "is_hidden": false
    },
    "created_at_ts": "2022-11-13T17:01:32+01:00",
    "created_time_ago": "13/11/2022"
  }
]
```

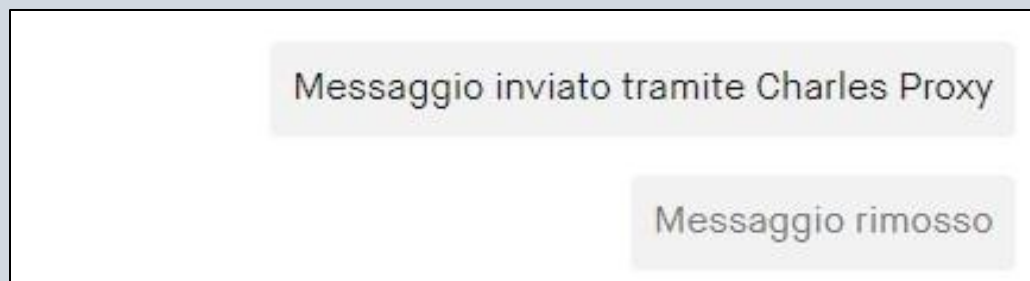
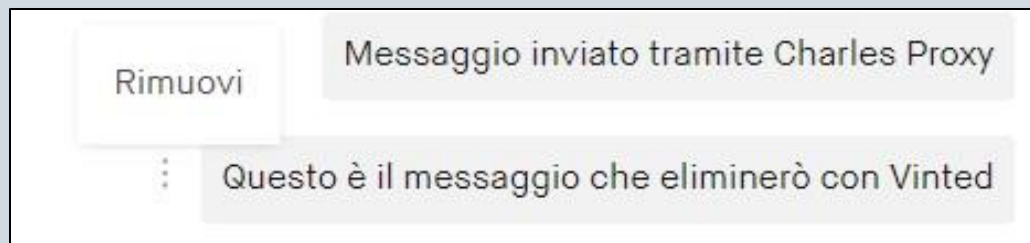
Ogni qualvolta l'utente invia un messaggio viene effettuata una operazione **HTTP** chiamata **GET** che restituisce l'intera chat con quell'utente e una **POST** con la quale riusciamo a vedere il messaggio che abbiamo appena inviato.

E' possibile visualizzare interamente ogni conversazione avviata dal nostro profilo e sapere se dall'altra parte, l'utente destinatario dei nostri messaggi stia rispondendo o meno da cellulare.

```
{
  "reply": {
    "body": "Messaggio inviato tramite Charles Proxy",
    "photo_temp_uuids": null
  }
}
```



*Ci siamo chiesti se fosse possibile manomettere i messaggi che l'utente stesse inviando tramite le stesse operazioni **HTTP** illustrate nella slide precedente. Attraverso un'operazione di **POST** siamo riusciti ad inviare nuovi messaggi ad un altro utente con cui avevamo già avviato una conversazione, direttamente da Charles Proxy*



Vinted fornisce inoltre la possibilità ai suoi utenti di eliminare un messaggio da loro inviato in qualunque momento lo si voglia. Una volta avvenuta l'eliminazione del messaggio esso comparirà nella chat come "Messaggio rimosso".


Overview	Contents	Summary	Chart	Notes
<pre>:method DELETE :authority www.vinted.it :scheme https :path /api/v2/conversations/6187290644/replies/17250368420 sec-ch-ua "Google Chrome";v="107", "Chromium";v="107", "Not= accept application/json, text/plain, */* x-csrf-token s9sfMNLJ_ZTfIDDefhu8CP0sfPieVI9XJ57mQlpFGbG96VbY accept-language it-fr sec-ch-ua-mobile ?0</pre>				

```
"entity_type": "message",
"entity": {
  "body": "Messaggio rimosso",
  "photos": [],
  "user_id": 58224596,
  "sent_via_mobile": false,
  "id": 17250368420,
  "reaction": null,
  "is_hidden": true
},
```

*Quando un messaggio viene eliminato da Vinted notiamo che viene effettuata un'operazione HTTP chiamata **DELETE**. Osservando il campo path ci siamo accorti che l'ultima stringa corrisponde all'id del messaggio appena eliminato.*

```
"entity_type": "message",
"entity": {
  "body": "Questo è il messaggio che eliminerò tramite Charles Proxy",
  "photos": [],
  "user_id": 58224596,
  "sent_via_mobile": false,
  "id": 17250758982,
  "reaction": null,
  "is_hidden": false
},
```

Compose

DELETE 

<https://www.vinted.it/api/v2/conversations/6187290644/replies/17250758982>

*Abbiamo quindi capito che fosse possibile eliminare qualunque messaggio da noi inviato semplicemente conoscendone l'identificativo e inserendolo nel campo path di una nuova operazione **DELETE**. Ricordiamo che l'id di ogni messaggio è facilmente recuperabile nel riepilogo della chat che viene visualizzato con una **GET** ad ogni nuovo messaggio che inviamo o riceviamo.*

```
:method GET
:authority www.vinted.it
:scheme https
:path /api/v2/conversations/6299942724
sec-ch-ua "Not?A_Brand";v="8", "Chromium";v="108", "Google
accept application/json, text/plain, */*
x-csrf-token ZxrTLS9QMT0oLIQng-k44ffb42fX6NmcTfgKqefSgVZ
accept-language it-fr
sec-ch-ua-mobile ?0
```

Compose	
DELETE ▾	https://www.vinted.it/api/v2/conversations/6299942724

*Dal momento in cui Vinted restituisce tramite una **GET** le conversazioni avviate dall'utente, abbiamo provato ad effettuare un'operazione di **DELETE** sullo stesso URL al quale è stata restituita una conversazione.*



*Ciò che accade effettuando l'operazione di **DELETE** è che la conversazione viene completamente eliminata dal nostro elenco delle chat su Vinted. I messaggi al suo interno non sono stati ovviamente eliminati e sarà possibile recuperarli solo se l'utente ci ricontatterà utilizzando quella stessa chat. In caso contrario sarà impossibile per noi recuperarla da Vinted. A sinistra è possibile osservare l'elenco delle chat prima della **DELETE**, a destra se ne osservano i risultati.*



Wallapop è una compagnia spagnola fondata nel 2014 utilizzata per lo scambio di beni usati. Nel 2015 è stata citata come la startup con i ricavi più alti in Spagna con 1 miliardo di dollari di transazioni completate utilizzando l'app.

Nel nostro paese Wallapop ha avuto larga diffusione soprattutto negli ultimi anni. Lo slogan con il quale si è presentato al nostro paese è stato “Se non lo usi, vendilo”. Qual è il livello di sicurezza fornito da Wallapop?

AUTENTICAZIONE

Il primo aspetto analizzato è stato quello relativo all'autenticazione. In particolar modo, abbiamo cercato di capire se utilizzando Charles Proxy al momento dell'autenticazione su Wallapop fosse possibile visualizzare le credenziali appena inserite. Wallapop fornisce tre metodi di accesso: quello attraverso il proprio account Facebook, tramite l'account Google oppure mediante la più classica combinazione email/username e password.



```
{
  "emailAddress": "XXXXXXXXXXXXXXXXXXXX",
  "password": "XXXXXXXXXX",
  "metadata": {
    "recaptchaToken": "03AEkXODCbIa-qk9Ju4bl06iUb55OMzAY32cjWALWS-F",
    "sessionId": "203d49b6-1ae3-49a9-99bb-3adcd98c3d"
  }
}
```

Informazioni visualizzate una volta effettuato l'accesso con username e password

```
{
  "token": "M6PhWSEiqHCJLlHIE9PfrEasODvYFom4B7DsxFXKuC7iYPUxCZizCjpgwt7Cx12",
  "resetToken": "6GS7ctceIganyjnDsJX6J0tANL8otQuA98bVvq0t6CC3vG7aYhCP4GgbEd",
  "expirationDate": "Fri Feb 24 16:57:27 GMT 2023",
  "registerInfo": {
    "userId": 430184747,
    "userUUID": "ejk4m207wrzx",
    "idUser": 430184747
  }
}
```

Informazioni visualizzate una volta effettuato l'accesso con un account Google

```
{
  "token": "kMNADrLdwQ5FMk5HAexwRqNIC6juszepoIbkJ2CIW8pxlDUIs7C8VQJaJw3MO",
  "resetToken": "YpT4VscQxLi2QMM4ivJipUmWJlWiqfHAMGBsmpmueE2o8sTUVtgMORlsNb",
  "expirationDate": "Fri Feb 24 16:59:31 GMT 2023",
  "registerInfo": {
    "userId": 430184747,
    "userUUID": "ejk4m207wrzx",
    "idUser": 430184747
  }
}
```

Informazioni visualizzate una volta effettuato l'accesso con un account Facebook

Qualora l'utente si registrasse alla piattaforma tramite Google/Facebook, al momento dell'accesso saranno visualizzabili soltanto le informazioni sui token di login e sugli **UserUID** e **UserUUID**; al contrario, le credenziali di accesso saranno visibili all'interno della **POST** che viene inviata a Wallapop.

COSA POSSO VEDERE DEGLI ALTRI?

Le informazioni che **Wallapop** salva dei suoi utenti sono molteplici. Ci siamo quindi chiesti quali informazioni sensibili legate agli altri utenti potessimo vedere. Per dati sensibili, in questo contesto, si intende tutto ciò che non sarebbe possibile vedere con un normale utilizzo dell'app/sito web.



```
{  
  "scoring_stars": 0.0,  
  "validations": {  
    "email": true,  
    "mobile": true,  
    "facebook": false,  
    "google_plus": false,  
    "linkedin": false,  
    "gender": true,  
    "location": false,  
    "picture": false,  
    "level": "verified",  
    "birthday": true  
  },  
  "activity_level": "unknown"  
}
```

Come prima cosa, cercando un utente qualunque da Wallpop, possiamo capire se ha effettuato l'accesso tramite email, Facebook o Google e possiamo sapere se ha verificato il suo numero di telefono. In questo caso, l'utente accede tramite la sua email ed ha verificato il suo numero di telefono.

```
{
  "id": "9jd2vx5mgn6k",
  "title": {
    "original": "Apple Ipad mini"
  },
  "description": {
    "original": "Ipad mini 5th generazione 2019 mo"
  },
  "taxonomy": [{
    "id": "15000",
    "name": "Informatica e Elettronica",
    "icon": "pc"
  }, {
    "id": "10135",
    "name": "Altro"
  }],
  "type": "consumer_goods",
  "user": {
    "id": "pj9y4yx42v6e"
  }
}
```

```
"supports_shipping": {
  "flag": true
},
"shipping": {
  "item_is_shippable": true,
  "user_allows_shipping": true
},
"hashtags": {
  "values": ["ipad", "tablet", "apple"]
},
"favorited": {
  "flag": false
},
"counters": {
  "views": 16,
  "favorites": 2,
  "conversations": 1
}
```

Cercando un oggetto a cui siamo interessati riusciamo a capire se il venditore ha già intrapreso una conversazione con qualcuno. In questo caso la voce conversations è pari a 1, il che significa che il venditore in questione era già stato contattato da un altro utente interessato all'oggetto messo in vendita.

COSA POSSO VEDERE DEL MIO ACCOUNT?

Successivamente ci siamo chiesti quali informazioni sensibili, relative all'account con il quale si effettua l'accesso, fossero visibili. Oltre alle informazioni mostrate in precedenza riguardo i profili degli altri utenti è stato possibile visualizzare informazioni ancora più delicate.




```
},
"location": {
  "approximated_latitude": 40.843968195966994,
  "approximated_longitude": 14.274969812353971,
  "full_address": "",
  "city": "Napoli",
  "zip": "80139",
  "country_code": "IT",
  "approxRadius": 1,
  "approximated_location": true,
  "title": "80139, Napoli"
},
"gender": "undefined",
"web_slug": "lucap-417608439",
"url_share": "http://p.wallapop.com/p/417608439?_pid=wi&uid",
"register_date": 1646510506000,
"featured": false,
"birth_date": -1262304000000,
"email": "lucapezzolla[REDACTED]@",
"first_name": "Luca",
"last_name": "Pezzolla",
"phone": "+[REDACTED]",
"has_accepted_terms": true,
"has_credentials_leaked": false
}
```

Se l'account con il quale accediamo ha collegati email e numero di telefono riusciamo a vederle senza alcun problema. Oltre a questo, possiamo reperire alcune informazioni circa la nostra geolocalizzazione, seppur non del tutto precise. Curioso ma vero, l'ultima flag ci permette di sapere se le nostre credenziali siano state o meno leakate.

```
{
  "id": "ed485b23-████████████████████",
  "iban": "IT48XXXXXXXXXXXXXXXXX6021",
  "owner_name": "Luca Pezzolla",
  "owner_last_name": "Pezzolla",
  "street": "Via ██████████",
  "flat_and_floor": "I ██████████",
  "postal_code": "80049",
  "city": "Somma Vesuviana",
  "country": "IT"
}
```

Se l'account con il quale accediamo ha collegati carta di credito e conto bancario, riusciamo a vedere diverse informazioni relative a queste ultime. Alcune cifre dell'IBAN, così come quelle del numero della carta di credito, vengono oscurate semplicemente attraverso delle X.

```
{
  "id": "6f0580af-████████████████████",
  "number_alias": "████████XXXXXX████████",
  "expiration_date": "████████████████████",
  "country": "ITA",
  "card_holder_name": "Luca Pezzolla",
  "status": "VALID"
}
```

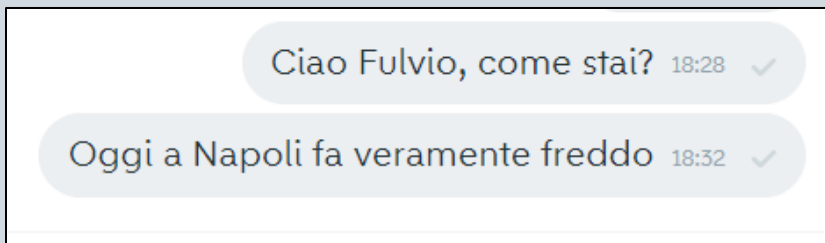
MESSAGGISTICA

Wallapop mette a disposizione una chat tra gli utenti in modo tale che questi possano chiedere informazioni ulteriori relativamente ad un prodotto in vendita a cui sono interessati oppure fare un'offerta diversa rispetto al prezzo di partenza.



```
    "messages": {  
      "messages": [{  
        "id": "8f297a83-bc31-4e9c-b050-7f10ab57f9d6",  
        "from_self": true,  
        "text": "Ah haha",  
        "timestamp": 1669481747207,  
        "status": "read",  
        "type": "text"  
      }, {  
        "id": "5ec8bf89-2246-44ed-af06-59a9bfefe5d0",  
        "from_self": false,  
        "text": "master",  
        "timestamp": 1669479695328,  
        "status": "read",  
        "type": "text"  
      }, {
```

Ogni qualvolta l'utente clicca sulla sua Inbox da Wallapop, Charles Proxy ci mostra il contenuto dell'operazione GET che restituisce tutte le conversazioni avviate dall'utente in questione.



*Se l'utente invia un messaggio tramite la chat di Wallapop, tramite Charles Proxy riusciamo a vedere il contenuto della **GET** che mostra i nuovi messaggi inviati e l'intera conversazione con l'altro utente. Non viene effettuata alcuna operazione di **POST**, per cui non è stato possibile modificare o inviare nuovi messaggi da Charles Proxy.*

```
"messages": {  
  "messages": [{  
    "id": "c5e15ff4-c9a2-4664-96a3-033a95d4c410",  
    "from_self": true,  
    "text": "Oggi a Napoli fa veramente freddo",  
    "timestamp": 1670002338252,  
    "status": "sent",  
    "type": "text"  
  }, {  
    "id": "f91ab71e-0e87-46db-8828-580ca565a1ld",  
    "from_self": true,  
    "text": "Ciao Fulvio, come stai?",  
    "timestamp": 1670002109772,  
    "status": "sent",  
    "type": "text"
```

Tuttavia, questo ci ha spinto a capire in che modo avvenisse la comunicazione tra noi client e i server di Wallapop. Ebbene, grazie a Burp, ci siamo resi conto che la comunicazione avviene tramite WebSocket, una tecnologia web che sfrutta una singola connessione **TCP** per aprire un canale di comunicazione full-duplex (ovvero una trasmissione bidirezionale).

```
<message xmlns="jabber:client" id="5ec8bf89-2246-44ed-af06-59a9bfefe5d0" to="36ewxo43kk6d@wallapop.com" from="
ejk4m207wrzx@wallapop.com/WEB_22536077183636" type="chat">
  <thread>
    3zln8x4o8p6x
  </thread>
  <request xmlns="urn:xmpp:receipts"/><body>
    mister
  </body>
</message>
```

Questo è il corpo di un messaggio inviato tramite websocket. Si noti la presenza di due indirizzi mail @wallapop.com, il cui identificativo alfanumerico che precede il dominio corrisponde all'id dell'account. Il corpo del messaggio è racchiuso tra i tag <body>, e nel nostro caso il messaggio inviato è «mister». Tale messaggio può essere tranquillamente modificato, grazie a software quali Burp, che intercettano la richiesta e sono in grado di cambiarne il contenuto. Non è però possibile né eliminare né modificare messaggi precedentemente inviati: di base, infatti, Wallapop non fornisce queste funzionalità.



Subito è tra le principali aziende di e-commerce dell'usato in Italia. Nata a Milano nel 2007, ad oggi è tra i primi 10 marchi online più visitati in Italia, con 11 milioni di utenti ogni mese.

Nel nostro paese, Subito si è pubblicizzata ufficialmente per la prima volta attraverso lo slogan: "I desideri si realizzano subito". Qual è, quindi, il livello di sicurezza fornito da Subito.it?

AUTENTICAZIONE

Il nostro primo approccio a **Subito** si è incentrato sul processo di autenticazione, possibile anche in questo caso tramite le solite tre modalità: Email/Password | Google | Facebook. Preannunciamo che, anche su Subito, è possibile vedere le credenziali di login se si sceglie la modalità di accesso canonica; al contrario, loggandosi tramite Facebook o Google, sarà visibile soltanto un link di redirecting ottenuto tramite una **GET**.



```
{
  "username": "XXXXXXXXXX",
  "password": "XXXXXXXXXX",
  "remember_me": true,
  "back": ""
}
```

Informazioni visualizzate una volta effettuato l'accesso con username e password

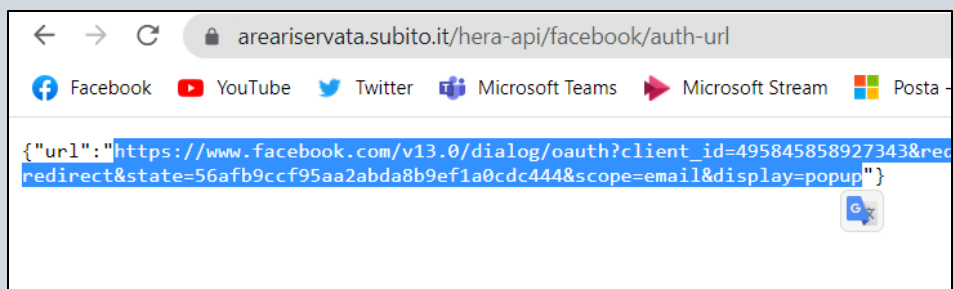
```
{
  "url": "https://accounts.google.com/o/oauth2/v2/auth?scope=op
}
```

Link visualizzato una volta effettuato l'accesso con Google

```
{
  "url": "https://www.facebook.com/v13.0/dialog/oauth?client_id=495845858927343&redirect_
}
```

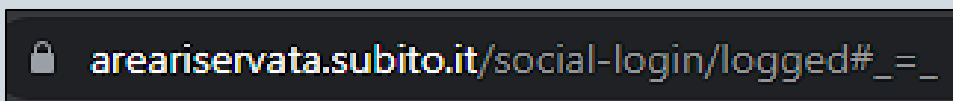
Link visualizzato una volta effettuato l'accesso con Facebook

Ci siamo quindi chiesti se fosse possibile riutilizzare il seguente link per accedere al medesimo account a cui esso è associato. La pagina nella quale viene restituito un nuovo link è <https://areariservata.subito.it/hera-api/facebook/auth-url> (nel caso di Google basta sostituire quest'ultimo al posto di Facebook). Ogni qualvolta aggiorniamo la pagina web su cui abbiamo visitato tale dominio, viene generato un nuovo link di accesso come se avessimo effettuato il login/logout da **Subito**. Copiando e incollando tale link in una nuova pagina web riusciamo ad effettuare l'accesso al nostro account **Subito** SOLO se avevamo già effettuato l'accesso a quell'account su quel determinato browser. In effetti, il link che abbiamo ottenuto è solamente una redirectione all'account Facebook/Google con il quale effettuiamo l'accesso.



Copiamo quindi il link di accesso come spiegato in precedenza e incolliamolo nella barra in alto del browser.

La pagina ci reindirizzerà nella nostra area riservata, la quale avrà al centro una schermata di caricamento che caricherà all'infinito. Se il link incollato non era scaduto, andando su Subito.it ci accorgeremo che siamo stati loggati senza aver effettuato l'accesso in maniera "manuale", ma solamente copiando e incollando il link di accesso.



COSA POSSO VEDERE DEGLI ALTRI?

Le informazioni che **Subito** salva dei suoi utenti sono molteplici. Ci siamo quindi chiesti quali informazioni sensibili legate agli altri utenti potessimo vedere. Per dati sensibili, in questo contesto, si intende tutto ciò che non sarebbe possibile vedere con un normale utilizzo dell'app/sito web.



In questo caso non abbiamo trovato informazioni sensibili rilevanti relative agli altri utenti della piattaforma. Tutte le informazioni che **Subito.it** restituisce tramite **GET** riguardano dei dati che sono già facilmente visibile tramite il semplice utilizzo dell'applicazione/sito web, come ultimo accesso, data d'iscrizione, id del profilo e così via.

COSA POSSO VEDERE DEL MIO ACCOUNT?

Successivamente ci siamo chiesti quali informazioni sensibili, relative all'account con il quale si effettua l'accesso, fossero visibili. Oltre alle informazioni mostrate in precedenza riguardo i profili degli altri utenti, è stato possibile visualizzare informazioni ancora più delicate.



```
{
  "status": "Not Found",
  "errors": [{
    "error_code": "METHODS:not-found",
    "info": "resource not found"
  }],
  "request_id": "0AD87023:9494_0AD81C1C:1F90_638DE441_21FF8D76:000E",
  "code": 404
}
```

```
{
  "hyperwallet_id": "usr-[REDACTED]",
  "address": "Via [REDACTED]",
  "city": "Somma Vesuviana",
  "province": "NA",
  "country": "IT",
  "postal_code": "80049",
  "private_info": {
    "first_name": "Luca",
    "last_name": "Pezzolla",
    "date_of_birth": "2001-05-14"
  },
  "is_company": false,
  "can_receive_payments": true,
  "verification_in_progress": false,
  "selected_transfer_method": {
    "hyperwallet_token": "trm-[REDACTED]",
    "type": ""
  }
}
```

*Se l'utente controlla il conto bancario associato al suo account da Subito.it, attraverso Charles Proxy riusciamo a vedere alcune informazioni che ci vengono restituite tramite una **GET**. Tra queste troviamo le informazioni relative all'utente intestatario del conto ma non riusciamo a vedere nessuna cifra del suo **IBAN**.*

Pagamenti

Metodi di ricezione

Scegli dove ricevere quello che guadagni.

PREDEFINITO



PayPal

[Redacted]

Scollega

Cambia



Conto bancario

[Redacted]

Scollega

Cambia

*A differenza di Vinted e Wallapop, **Subito.it** permette anche di collegare al proprio account un conto Paypal con il quale effettuare pagamenti. Ciononostante, non è stato possibile reperire nessuna informazione a tal proposito attraverso gli strumenti utilizzati.*

MESSAGGISTICA

Subito mette a disposizione una chat tra gli utenti in modo tale che questi possano chiedere informazioni ulteriori relativamente ad un prodotto in vendita a cui sono interessati oppure fare un'offerta diversa rispetto al prezzo di partenza.



```

{
  "_links": {
    "conversations": [{
      "href": "https://subito.messaging.advgo.net/api/hal/112810583/conversations"
    }],
    "messages": [{
      "href": "https://subito.messaging.advgo.net/api/hal/112810583/conversations/r
    }],
    "self": {
      "href": "https://subito.messaging.advgo.net/api/hal/112810583/conversations/r
    }
  },
  "conversationId": "nYV5inXIiddQ2ufHww8p5K-HeydECa937G3R1Ccu37YL6sTGTtJFBCRDndAOPf",
  "itemId": "ad5125335781ist467529168",
  "itemType": "ad",
  "lastMessageAttachmentsCount": 0,
  "lastMessageDate": "2022-12-03T17:19:27+0000",
  "lastMessagePreview": "No è in ottimo stato",
  "pageHash": "1XKkWE01StNMmrUQ-NEqdyQPshJgmRyC2UXhphrfDC0oD1Y9cl2sCW3RxpniTGzxcajK",
  "partnerId": "113021664",
  "partnerName": "Alessandro Giuliani",
  "partnerProfilePictureUrl": "",
  "subject": "Nuovo messaggio per Armadio 6 ante (ID:467529168)",
  "unseenCounter": 1,
  "integrations": [],
  "realtimeContext": {
    "presenceStatus": "OFFLINE",
    "jid": "113021664_subito@xmpp.messaging.advgo.net"
  }
}

```

*Presence periodica relativa all'area messaggi, restituita tramite **GET**, che ci informa sui messaggi ricevuti, sullo stato del mittente (ONLINE o OFFLINE, seppur non precisissimo per via del polling di 12 secondi e visualizzabile pur non chattando con lui) e su altre informazioni più o meno rilevanti.*

```
{
  "clientId": "178da490-922e-4756-87db-d08a75f04897",
  "text": "Messaggio inviato con Charles",
  "attachments": [],
  "type": "ApiTextMessage"
}
```

POST "tipo" di Subito per l'invio di messaggi. E' possibile inviarne di nuovi tramite Charles Proxy ma non modificare o cancellare quelli già esistenti: Subito, d'altronde, non consente questa funzionalità di base.

```
{
  "id": "380d0d30-732f-11ed-9109-0a63b8bd67db",
  "text": "Messaggio inviato con Charles",
  "type": "ApiTextMessage",
  "typeAttributes": {},
  "date": "2022-12-03T17:23:35+0000",
  "read": true,
  "partnerRead": false,
  "outgoing": true,
  "attachments": [],
  "clientId": "178da490-922e-4756-87db-d08a75f04897",
  "notificationData": null
}
```

Conferma automatica, tramite una GET, di avvenuto invio del messaggio.