

Guida della vulnerabilità Account Takeover

Introduzione

Questa è la guida della vulnerabilità di tipo **Account Takeover**, seguendo questa guida riuscirai a sfruttare la vulnerabilità all'interno di HackerLab.

Questo tipo di vulnerabilità permette ad un malintenzionato di poter prendere il controllo completo ad un account di un'altra persona registrata all'interno di una determinata piattaforma.

Requisiti

- Browser (Nella guida viene utilizzato Chrome)
 - o <https://support.google.com/chrome/answer/95346>

Guida

Per sfruttare questa vulnerabilità si dovrà conoscere l'indirizzo email di un utente registrato all'interno della piattaforma web. Per ricavare un indirizzo email registrato puoi utilizzare la vulnerabilità documentata "Broken Authentication" oppure utilizzare il seguente indirizzo email: filippo.finke@samtrevano.ch. Per sfruttare questa vulnerabilità si sfrutterà quindi il recupero password tramite email.

Per capire come funziona la vulnerabilità crea un account all'interno del sito web e registrati utilizzando una email al quale hai accesso e che puoi ricevere email. Una volta creato l'account effettua il logout e recati nella schermata di recupero password. Ti basterà premere il pulsante "Password dimenticata?" nella schermata di login.

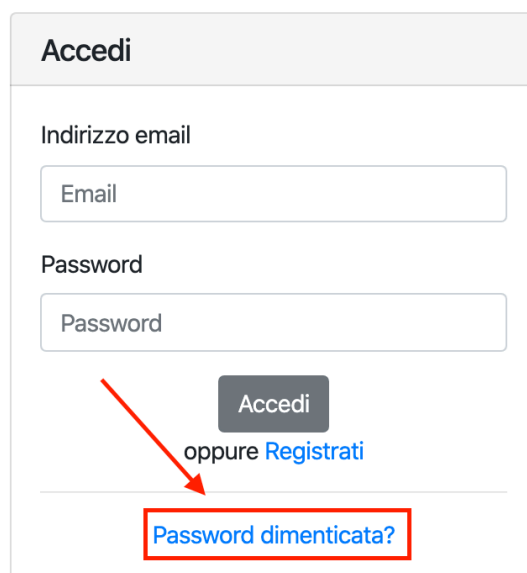
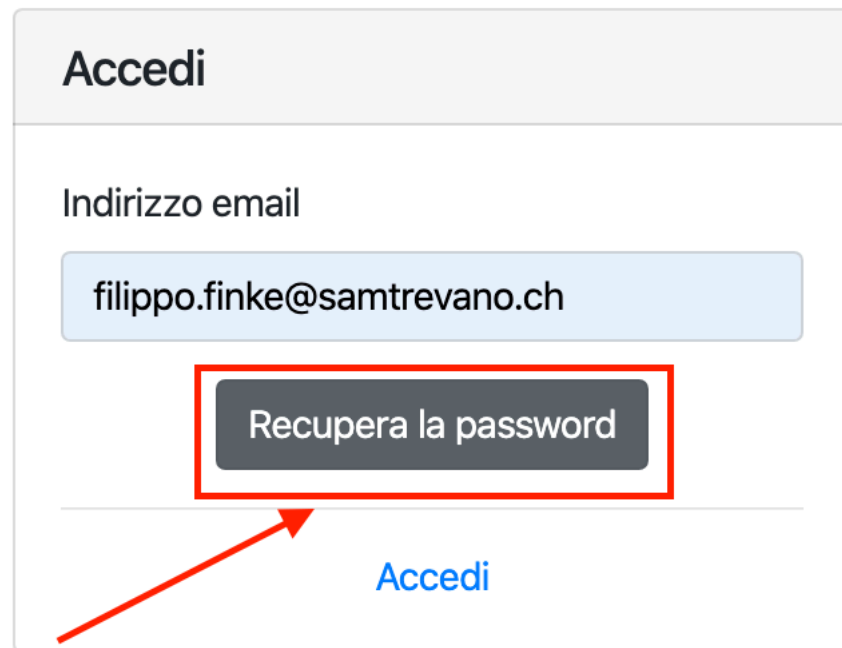


Figura 1 Accedere alla sezione di recupero password

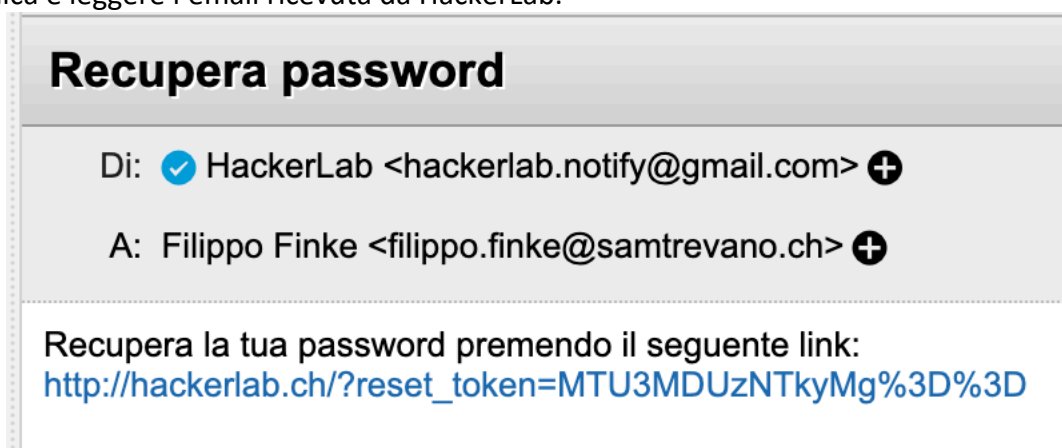
Una volta nella sezione di recupero password ti basterà inserire l'indirizzo email dell'account precedentemente creato e richiedere il recupero.



The screenshot shows a web form titled "Accedi" (Login). It contains a label "Indirizzo email" (Email address) above a text input field containing "filippo.finke@samtrevano.ch". Below the input field is a button labeled "Recupera la password" (Reset password), which is highlighted with a red rectangular border. A red arrow points from the "Accedi" link below the form to the "Recupera la password" button.

Figura 2 Richiedere il recupero password.

Una volta richiesto il recupero password sarà sufficiente andare nella propria casella di posta elettronica e leggere l'email ricevuta da HackerLab.



The screenshot shows an email interface with the title "Recupera password". The sender is "Di: HackerLab <hackerlab.notify@gmail.com>". The recipient is "A: Filippo Finke <filippo.finke@samtrevano.ch>". The body of the email contains the text: "Recupera la tua password premendo il seguente link:" followed by a blue hyperlink: http://hackerlab.ch/?reset_token=MTU3MDUzNTkyMg%3D%3D.

Figura 3 Email di recupero.

Come possiamo notare nell'email di recupero è presente un token, in questo caso `MTU3MDUzNTkyMg%3D%3D`. Il codice di recupero se riformattato normalmente sostituendo i caratteri codificati per l'url diventa `MTU3MDUzNTkyMg==`. Grazie a queste informazioni possiamo determinare il tipo di codifica che è stato utilizzato, in questo caso basandoci sugli uguali finali possiamo assumere sia del testo codificato in base64. Eseguendo quindi la decodifica della stringa

(ho utilizzato il sito <https://base64decode.org> per eseguire la decodifica) otteniamo la seguente stringa composta unicamente da numeri: **1570535922**.

Per capire che cosa rappresenta questo numero ho quindi richiesto un secondo recupero password seguendo la stessa procedura descritta precedentemente. Questa volta il token di recupero è stato il seguente: **MTU3MDUzNjl1MQ==** ho quindi proceduto a decodificare anche questo codice ed ho ottenuto il seguente valore: **1570536251**. Possiamo quindi notare che i due valori sono molto simili. Ho quindi sottratto i due valori e ottenuto il seguente risultato: **329** che convertito in minuti diventano circa 5 minuti e mezzo. Ho guardato quindi quando ho ricevuto le due email e possiamo notare che l'intervallo corrisponde.

<input type="checkbox"/> ☆ HackerLab	Recupera password	Oggi alle 14:04
<input type="checkbox"/> ☆ HackerLab	Recupera password	Oggi alle 13:58

Figura 4 Orario di ricezione delle email.

Possiamo quindi stabilire che il valore contenuto all'interno del token è l'orario in formato unix di quando è stato spedito il messaggio.

Ho quindi utilizzato il sito <https://epochconverter.com> per avere un ulteriore conferma:

1570535922	Timestamp to Human date	[batch convert]
------------	-------------------------	---------------------------------

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

GMT: Tuesday 8 October 2019 11:58:42

Your time zone: martedì 8 ottobre 2019 13:58:42 **GMT+02:00 DST**

Relative: 12 minutes ago

Figura 5 Orario trasformato.

Possiamo quindi confermare che il token è l'orario di quando è stato richiesto il recupero password dell'email.

Ora che abbiamo capito il funzionamento possiamo passare ad applicare la seguente vulnerabilità con l'email della vittima stessa.

Per eseguire la vulnerabilità sarà quindi necessario aprire la console da sviluppatore all'interno del proprio browser premendo il tasto **F12**, recarsi nella sezione "**Network**" e selezionare "**Preserve log**". In questo modo tutte le richieste che eseguiamo verranno tenute e mostrate nella console.

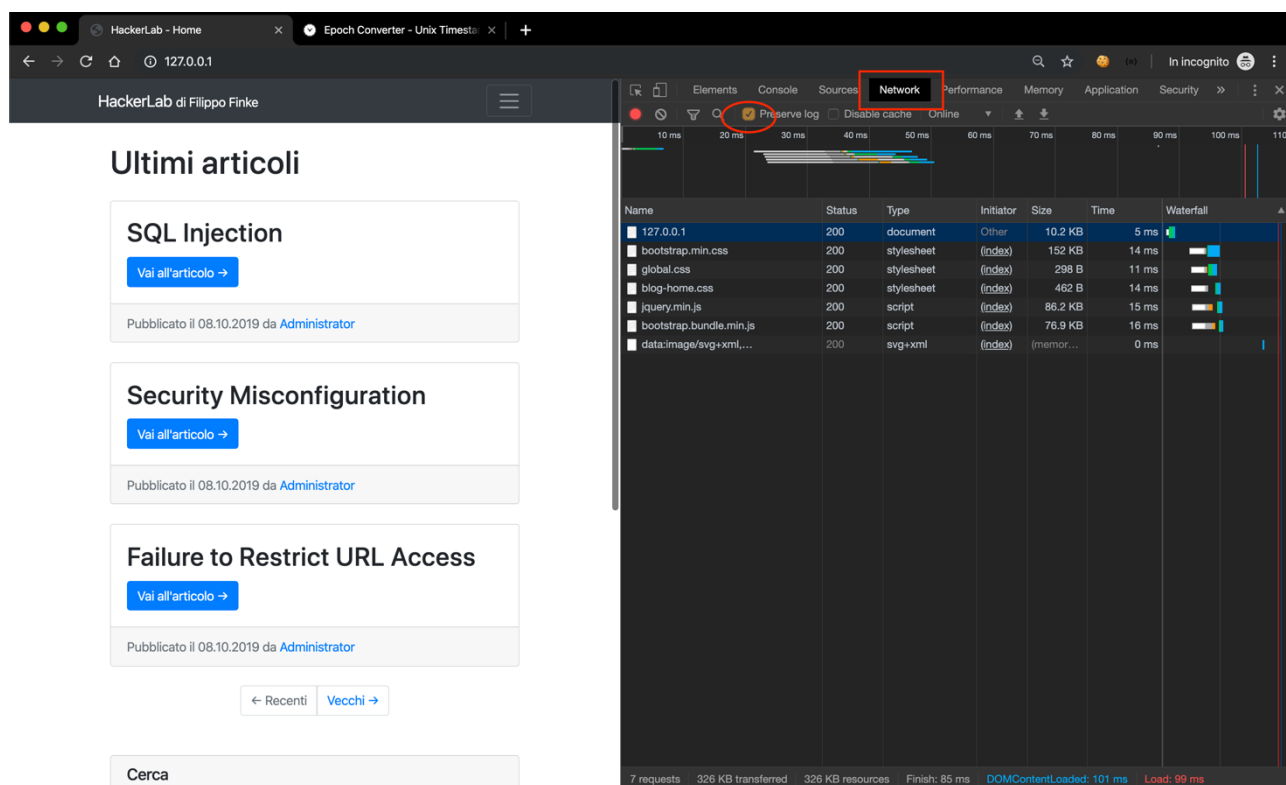


Figura 6 Impostare "Preserve log" nella console.

Una volta impostato il nostro ambiente, basterà eseguire il recupero password attraverso il form presente in HackerLab con l'email della vittima, in questo caso utilizzerò filippo.finke@samtrevano.ch.

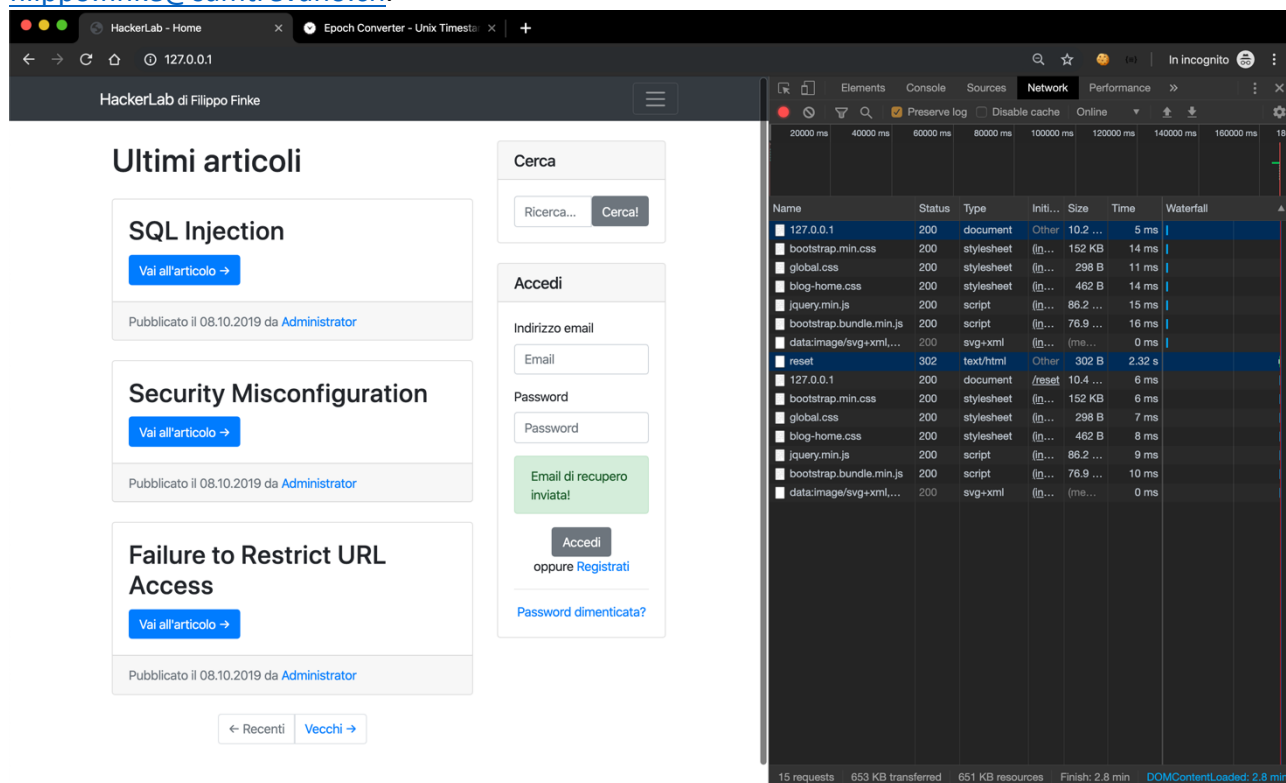


Figura 7 Invio recupero password.

Possiamo quindi notare sulla destra che sono apparse svariate richieste. Ci concentreremo sulla richiesta **reset** questo perché è la richiesta che richiede il recupero password. Quindi possiamo selezionarla per ispezionarne il contenuto.

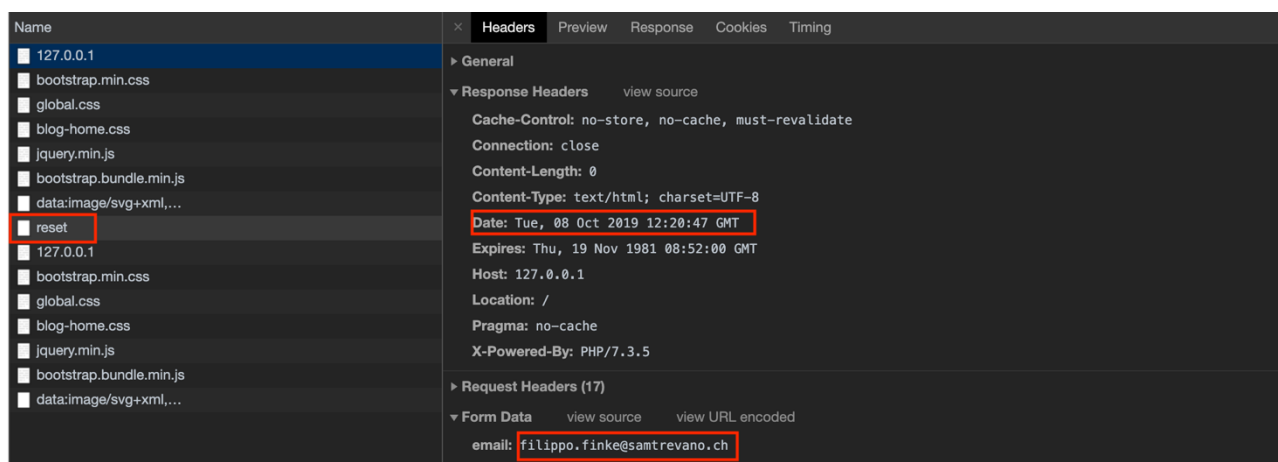


Figura 8 Contenuto della richiesta.

Possiamo quindi notare tutte le informazioni della richiesta stessa. Possiamo notare come sia presente l'email alla quale abbiamo richiesto il recupero e altre informazioni. Essendo la vulnerabilità basata sulla data della richiesta (come descritto in precedenza) possiamo notare un parametro **date**, questo parametro contiene la data di risposta del server. Essendo l'elaborazione del server molto veloce possiamo utilizzare questa data per la generazione del nostro token. Mi sono quindi recato sul sito <https://www.epochconverter.com/> per eseguire la conversione della data in formato unix timestamp.

Yr	Mon	Day	Hr	Min	Sec		
2019	-	10	-	8	12	:	20 : 47 GMT

Human date to Timestamp

Epoch timestamp: 1570537247

Timestamp in milliseconds: 1570537247000

Date and time (GMT): Tuesday 8 October 2019 12:20:47

Date and time (your time zone): martedì 8 ottobre 2019 14:20:47 GMT+02:00

Figura 9 Conversione della data.

Il timestamp è quindi **1570537247**, quindi per generare il token non ci resta altro che codificare il numero ricavato in base64. Ho quindi utilizzato <https://www.base64encode.org> per codificare la stringa ed ho ottenuto il seguente risultato: **MTU3MDUzNzI0Nw==**.

Una volta generato il token basterà procedere al percorso `/?reset_token=MTU3MDUzNzI0Nw==` e modificare la password con una a propria scelta.

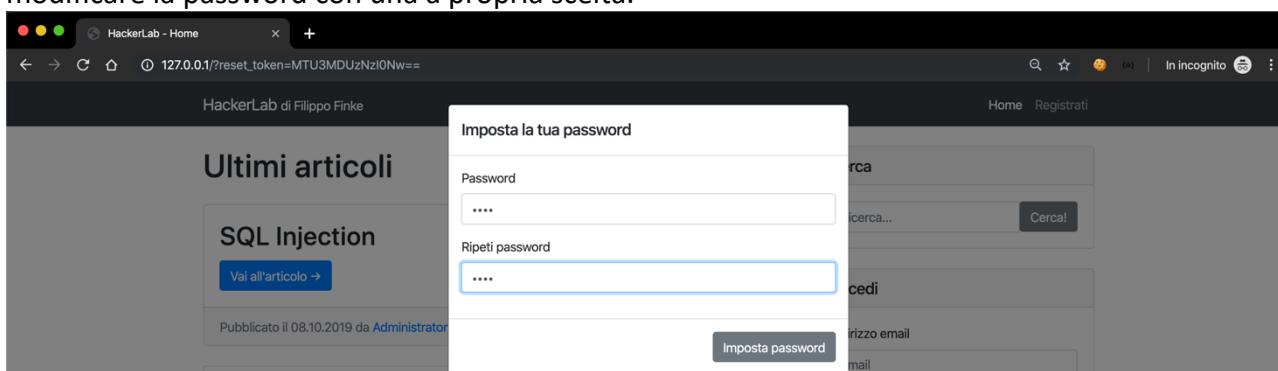
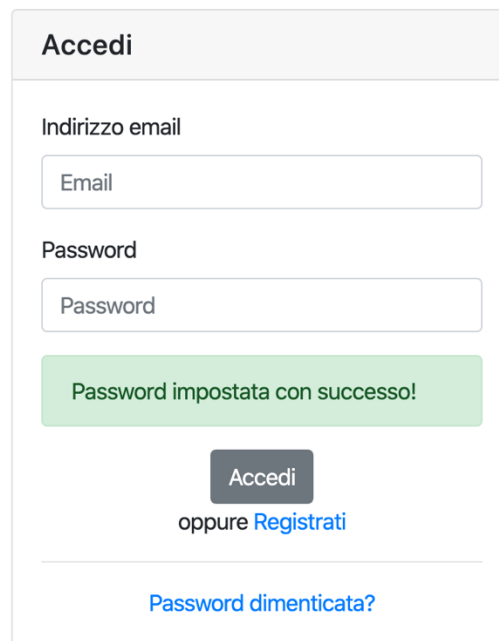


Figura 10 Impostazione nuova password.

Basterà quindi confermare la modifica della password. Nel caso il token sia errato basterà provare a generare il token con 1 secondo in più oppure in meno e riprovare. Ora sarà possibile accedere con l'email della vittima e la password impostata qualche secondo fa.



The screenshot shows a login form titled "Accedi". It contains two input fields: "Indirizzo email" with a placeholder "Email" and "Password" with a placeholder "Password". Below these fields is a green message box that says "Password impostata con successo!". At the bottom of the form, there is a dark grey button labeled "Accedi", followed by the text "oppure [Registrati](#)". A horizontal line separates this from a blue link at the bottom that says "Password dimenticata?".

Figura 11 Password resettata.



The screenshot shows a user dashboard titled "Accesso eseguito". Below the title, it says "Benvenuto **Filippo Finke**". At the bottom, there is a dark grey button labeled "Pubblica un articolo".

Figura 12 Accesso eseguito.

La vulnerabilità è quindi stata sfruttata. Questo tipo di falla è molto pericoloso in quanto permette ad un malintenzionato di accedere a tutti gli account presenti all'interno dell'applicativo web. Sfruttando per esempio questa vulnerabilità in combinazione con vulnerabilità di tipo "Insecure Direct Object References" e "Broken Authentication" potrà anche accedere all'applicativo come amministratore.