

»» Alege cui să trimiți documente și informații

Fiecare cont [SecureDrop](#) este total independent, iar documentele transmise pot fi descărcate doar de către jurnaliștii cărora le sunt expediate.

Toate organizațiile de media care utilizează SecureDrop oferă propriile recomandări specifice pentru utilizarea acestui program. Vă încurajăm să consultați pagina personalizată cu recomandări a unei organizații media înainte de a-i expedia documente sau informații.

Cele mai multe organizații își crează pagini web personalizate cu prezentarea soft-ului securizat, vizibile și accesibile pe pagina de start a site-ului oficial. De asemenea, puteți găsi [o listă incompletă a organizațiilor](#) care utilizează SecureDrop pe pagina informativă oficială a SecureDrop, administrată de Freedom of the Press Foundation.

»» Instalează browserul Tor

Fiecare cont SecureDrop are o interfață disponibilă publicului (*Source Interface*): un site unde sursele pot crea conturi anonime, pot expedia fișiere, mesaje și să verifice răspunsurile sau întrebările primite de la jurnaliști.

Fiecare pagină creată de organizația media este disponibilă numai prin intermediul *Tor Hidden Service* și folosește o adresă care se termină cu **".onion"**, accesibilă exclusiv prin intermediul browserului Tor.

Tor este o rețea anonimă care face dificilă monitorizarea rețelei și asocierea identității unui utilizator (*de exemplu, adresa de IP*) cu activitatea sa (*de exemplu, încărcarea informațiilor în SecureDrop*).

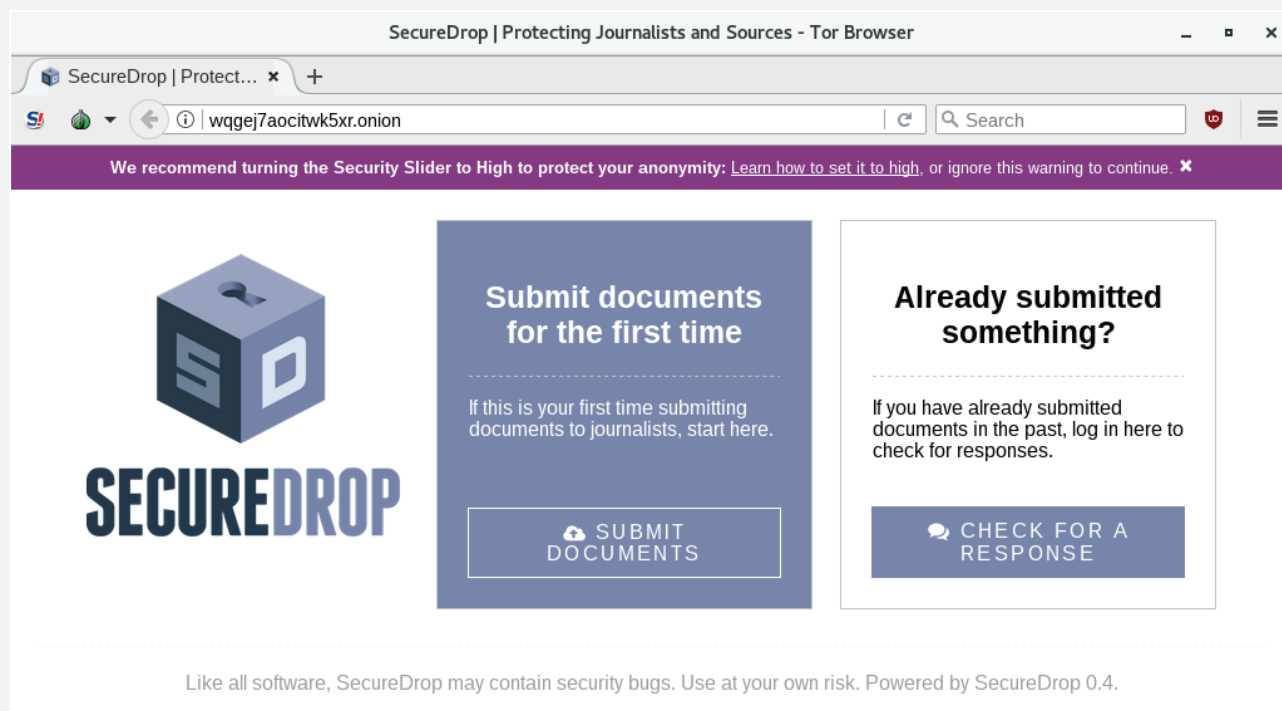
Cea mai ușoară și mai sigură modalitate de a utiliza Tor este descărcarea „pachetului Tor Browser” de pe [site-ul oficial Tor Project](#). Acest pachet include browserul Tor și o versiune modificată a browserului web Firefox, concepută pentru a vă proteja securitatea și anonimatul în timp ce utilizați Tor.

Odată ce ați instalat browserul Tor, introduceți adresa care se termină în **".onion"** pentru a accesa interfața-sursă (*Source Interface*) a organizației pe care doriți să o contactați (*de exemplu, aceasta este adresa RISE Moldova: 6lhmirnluwmvjw4z.onion*). Puteți găsi această adresă pe pagina personalizată a organizației (www.rise.md/leaks) sau pe pagina informativă a SecureDrop (*dacă aceasta a fost afișată acolo*).

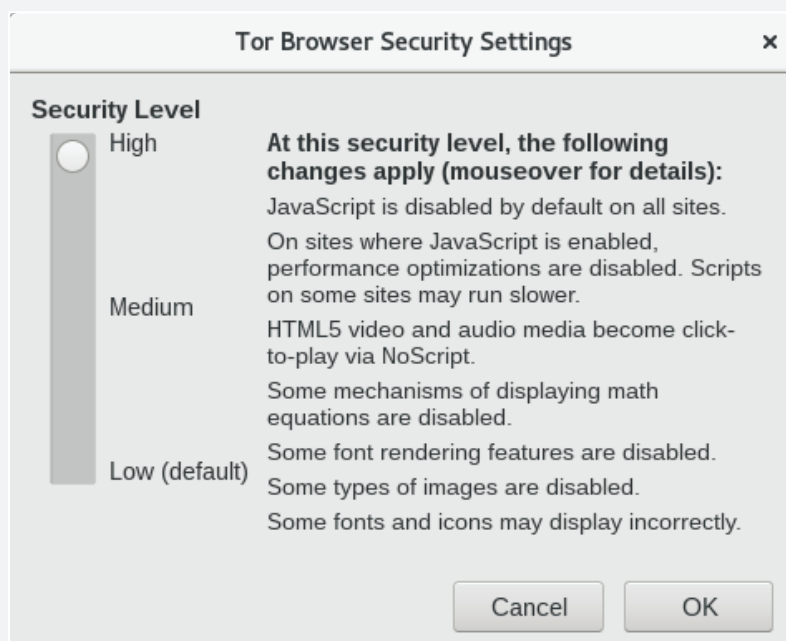
Browserul Tor vă ajută să vă ascundeți activitatea în rețea, însă acesta lasă urme (de instalare proprie) în computerul de pe care a fost accesat. Pentru un nivel mai ridicat de securitate, vă recomandăm să încărcăm un sistem de operare live, cum ar fi [Tails](#). Tails este conceput special pentru a rula pe computerul dvs. fără a lăsa urme ale activității dvs. și trasează automat navigarea prin Internet prin Tor, astfel încât să puteți accesa SecureDrop în siguranță.

»» Cum transmiți documente pentru prima dată?

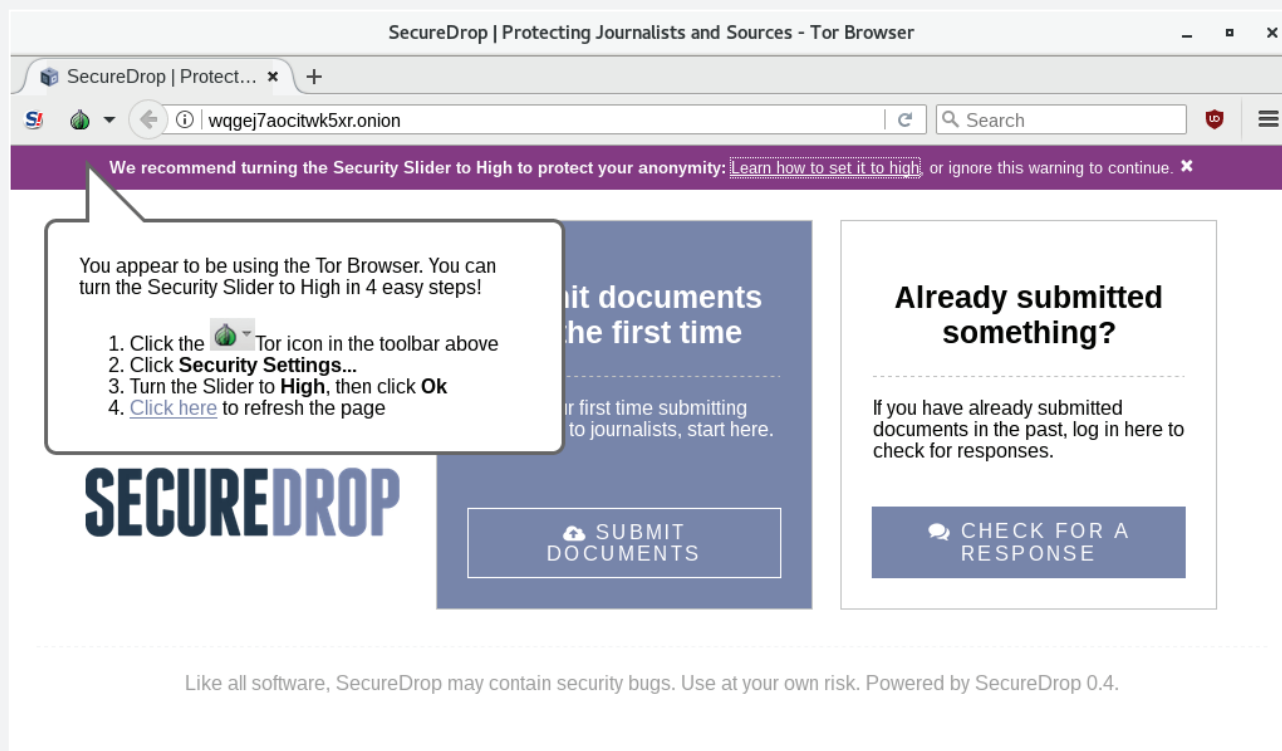
Deschideți browserul Tor și navigați la adresa ".onion" pentru interfața-sursă (*Source Interface*) de pe SecureDrop pe care doriți să o contactați. Pagina ar trebui să arate similar cu exemplul de mai jos, deși va avea probabil un logo specific organizației căreia îi expediați documentele.



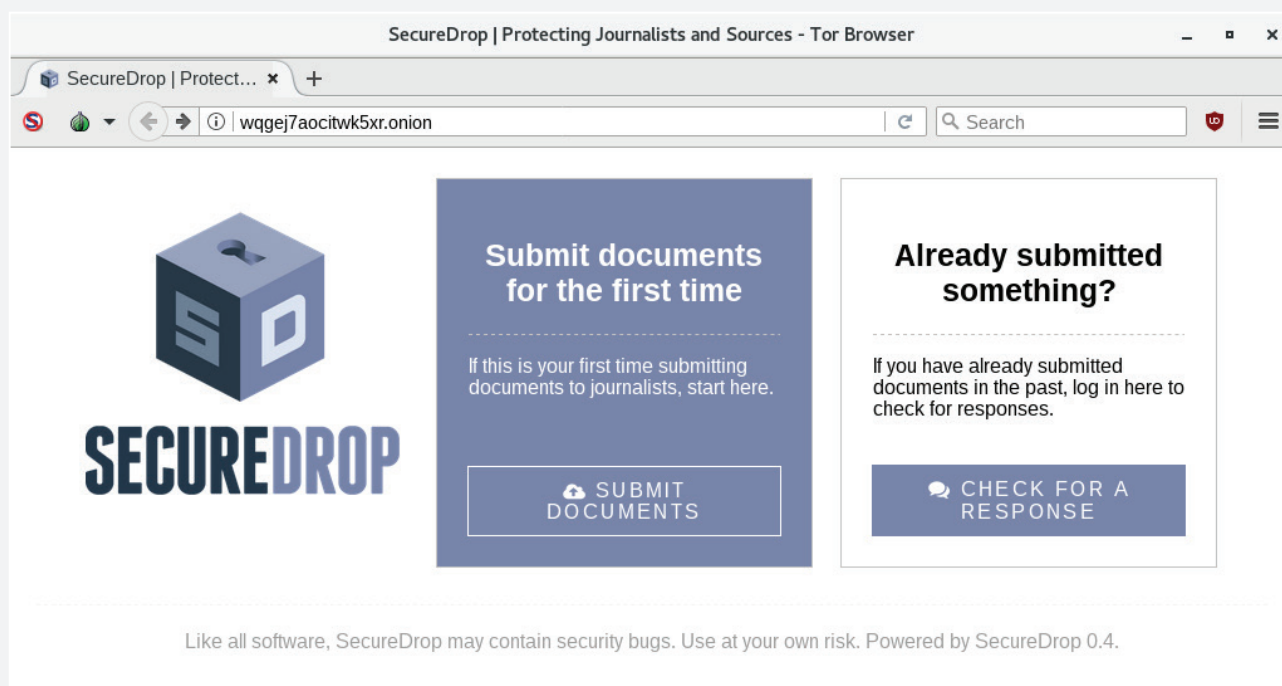
Dacă utilizați browserul Tor pentru prima dată, probabil că aveți *Javascript* activat și că nivelul de securitate pe care îl oferă browserul Tor este setat la "Low", adică scăzut. Dacă este așa, atunci în partea de sus a paginii va apărea un banner violet de avertizare care vă încurajează să dezactivați Javascript și să setați nivelul de securitate la "**High**" (înalt):



Apăsați pe modul **"Learn how"** în bannerul de avertizare. Astfel, va apărea un mesaj care va explica cum să dezactivați Javascript și să modificați gradul de securitate. Urmăriți instrucțiunile și pagina ar trebui să se actualizeze automat. Rețineți că acest lucru va schimba nivelul de securitate și va dezactiva *JavaScript* pentru fiecare pagină din browserul Tor, iar această setare va persista în toate sesiunile ulterioare pe Tor.



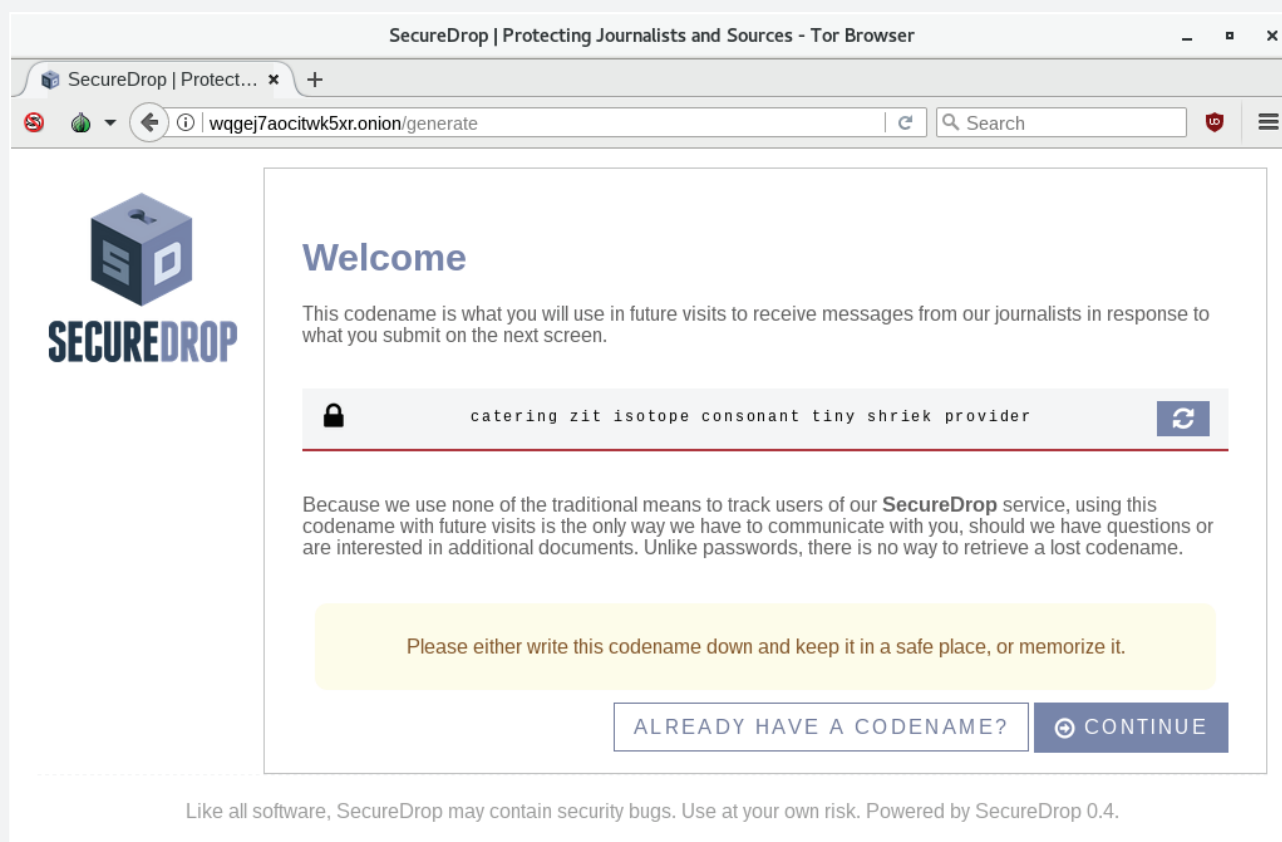
Pagina ar trebui să arate similar cu exemplul de mai jos. Dacă aceasta este prima dată când utilizați SecureDrop, faceți clic pe butonul **"Submit Documents"**.



Ar trebui să vedeți acum un ecran care să afișeze **un cod unic** pe care l-a generat SecureDrop. De exemplu, în imaginea de mai jos codul unic generat este - catering zit isotope consonant tiny shriek provider -, dar al dvs. va fi diferit. **ESTE EXTREM DE IMPORTANT SĂ SALVAȚI CODUL UNIC GENERAT DE SECUREDROP ȘI SĂ-L PĂSTRAȚI ÎN MOD SECRET.** După expedierea documentelor, veți avea nevoie de acest cod pentru a vă autentifica și a verifica răspunsurile.

Cea mai bună modalitate de a vă proteja codul este să-l memorați. Dacă nu-l puteți memora imediat, vă recomandăm să-l scrieți undeva și, pentru început, să-l păstrați într-un loc sigur, și treptat să-l memorați. **Odată ce l-ați memorat, ar trebui să distrugeți copia scrisă.**

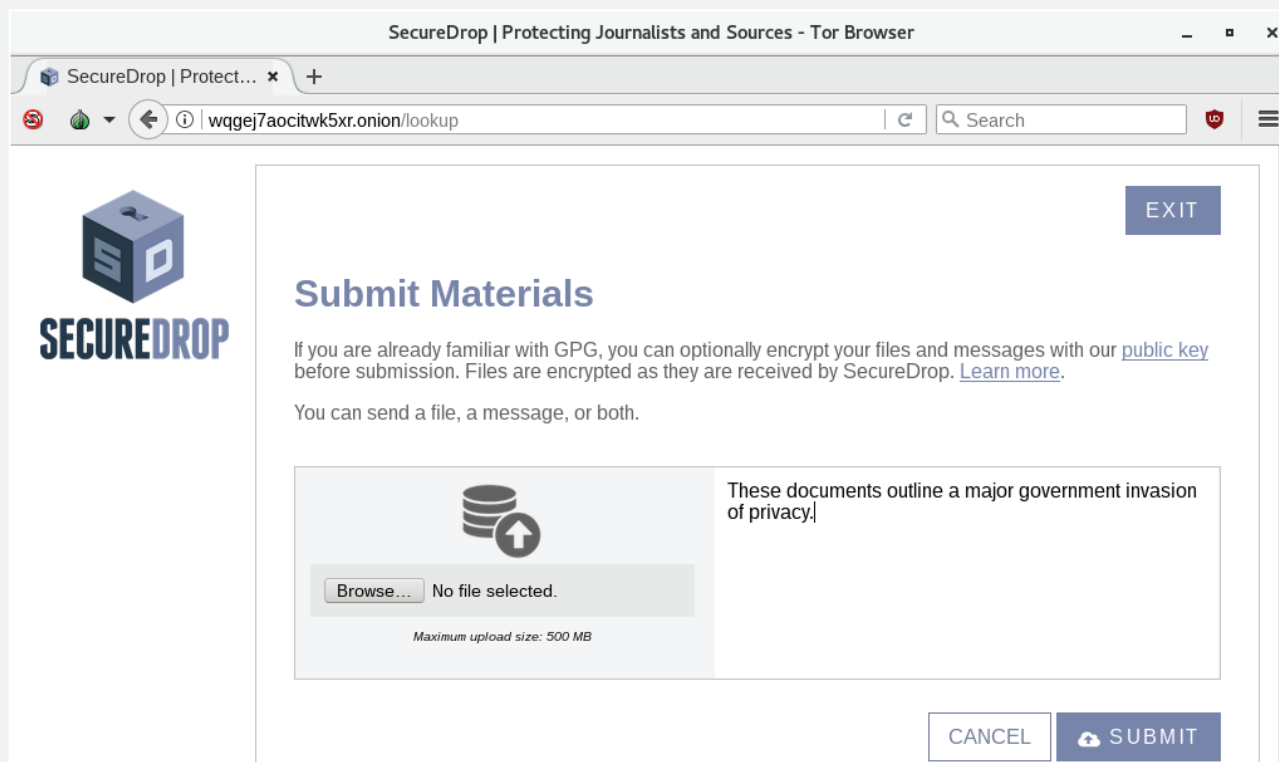
După ce ați primit codul unic și l-ați pus în siguranță, faceți clic pe **"Continue"**.



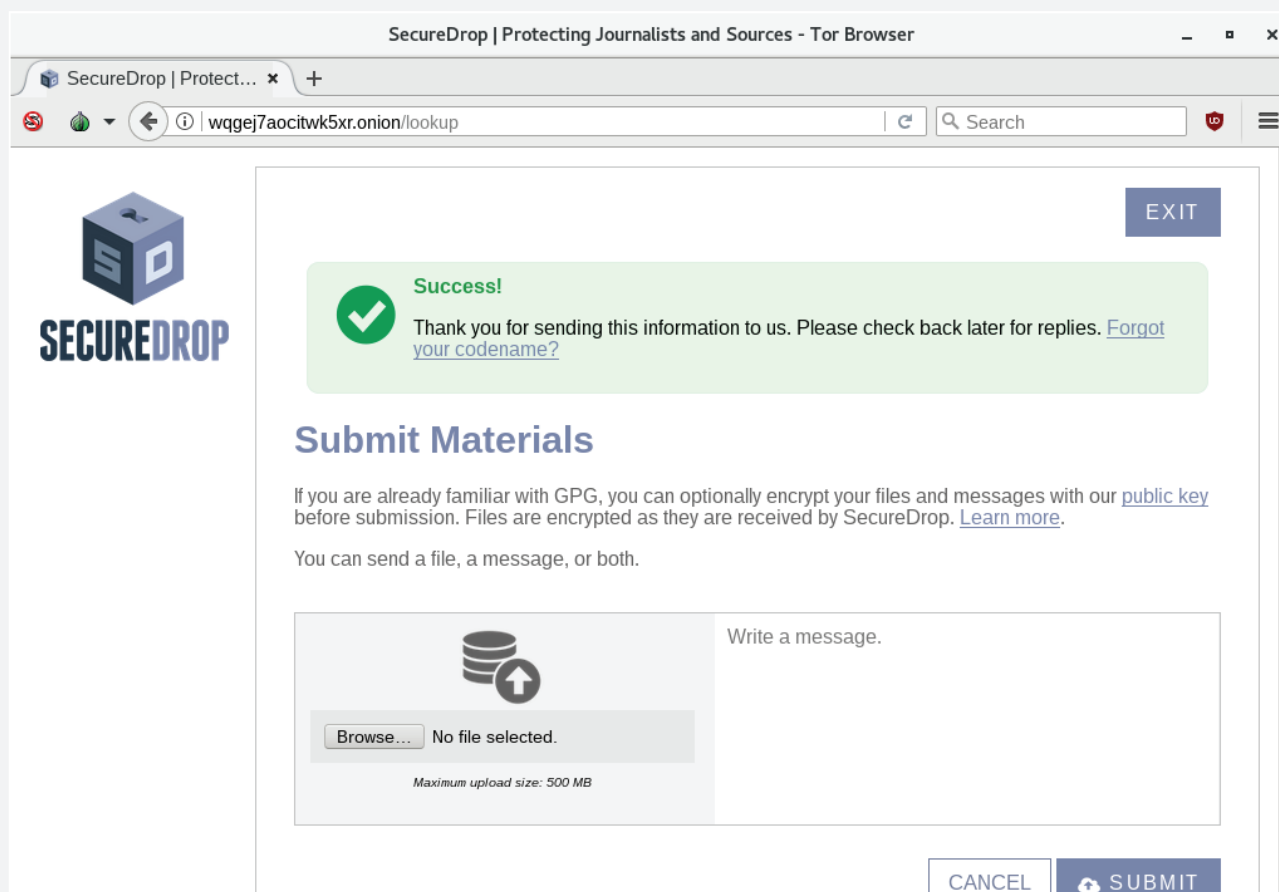
În continuare veți fi redirecționat spre interfața de unde puteți încărca un document și/sau scrie un mesaj pentru a-l expedia jurnaliștilor. Odată accesată, platforma vă permite să atașați doar un singur document per operațiune. Respectiv, în cazul în care aveți mai multe fișiere, combinați-le într-o arhivă de tip ".zip"

Dimensiunea maximă a fișierului expediat este, în prezent, de **500MB**. Dacă fișierele pe care doriți să le încărcați depășesc această limită, vă recomandăm să trimiteți un mesaj explicativ jurnaliștilor, astfel încât aceștia să poată configura o altă metodă de transfer al documentelor.

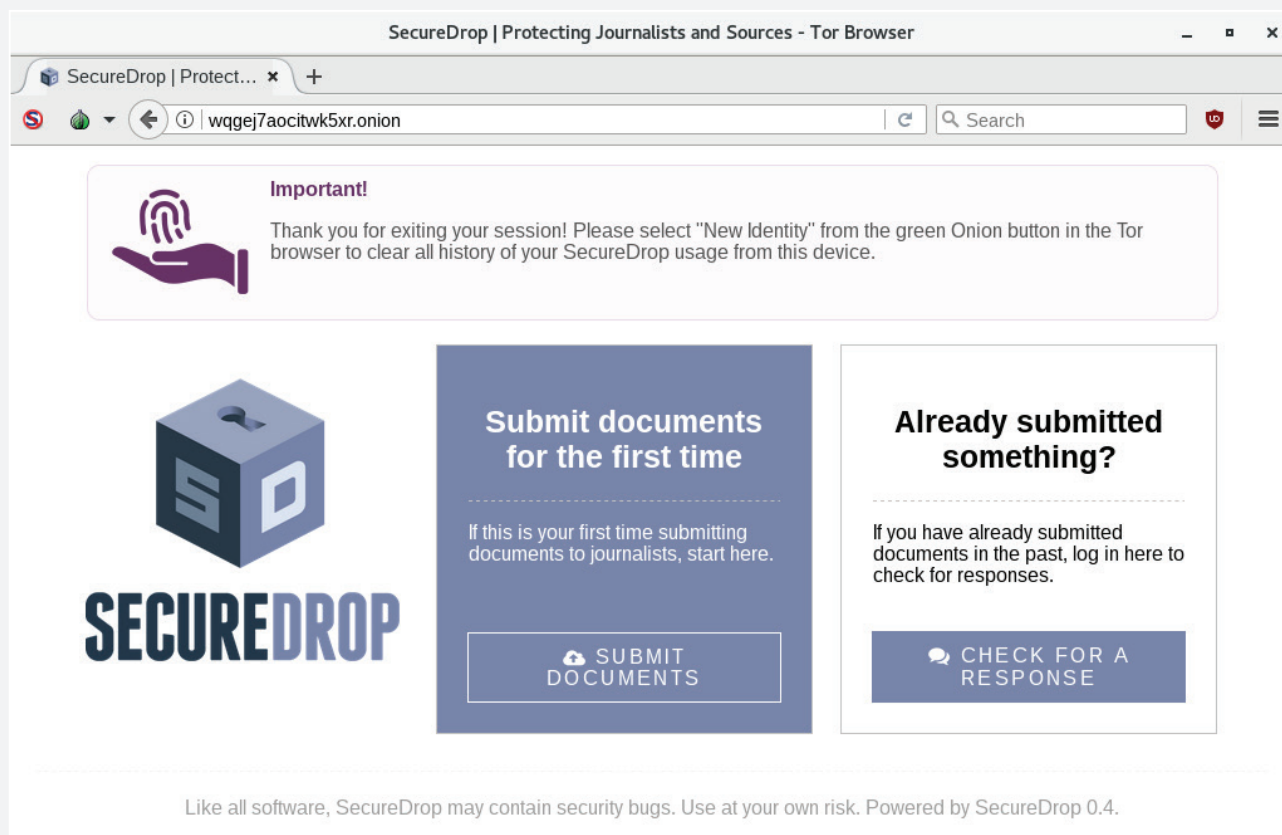
Când aplicația dvs. este gata, faceți clic pe **"Submit"**.



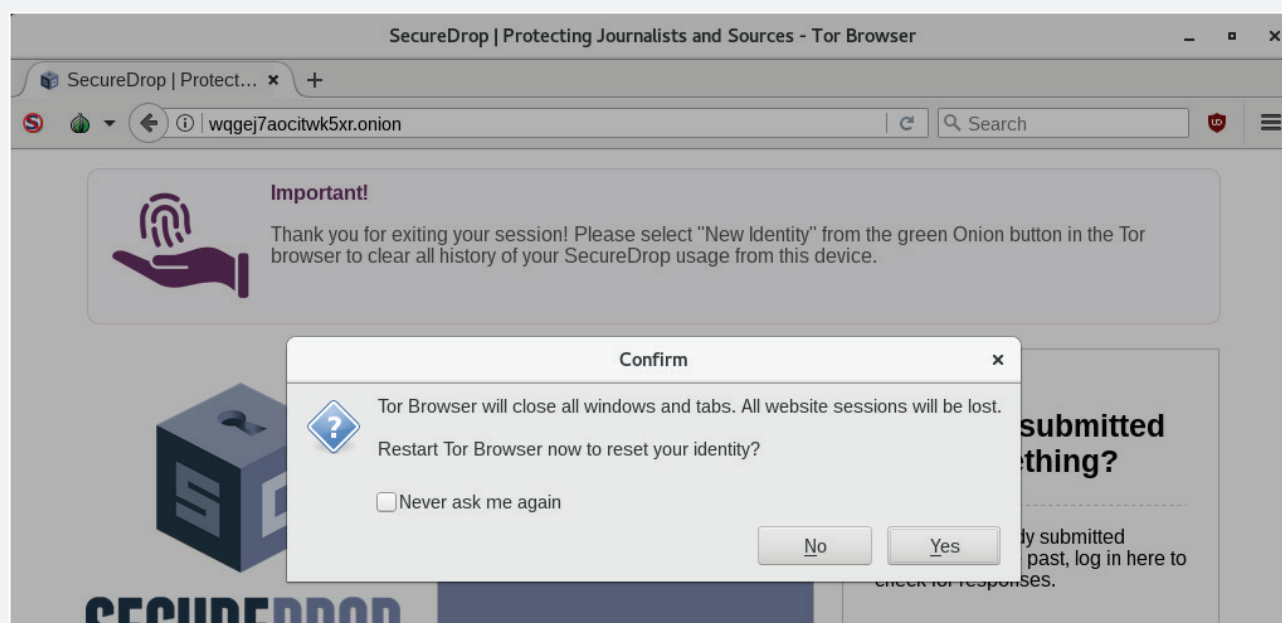
După ce apăsați **"Submit"**, ar trebui să apară o pagină de confirmare care să arate că mesajul și/sau documentele dvs. au fost expediate cu succes. Tot de pe această pagină puteți să efectuați și alte expedieri sau să vizualizați răspunsurile la mesajele anterioare.



După ce ați încheiat procedura de expediere a documentelor, asigurați-vă că ați salvat codul unic generat de SecureDrop și apoi apăsați butonul **"Exit"**:

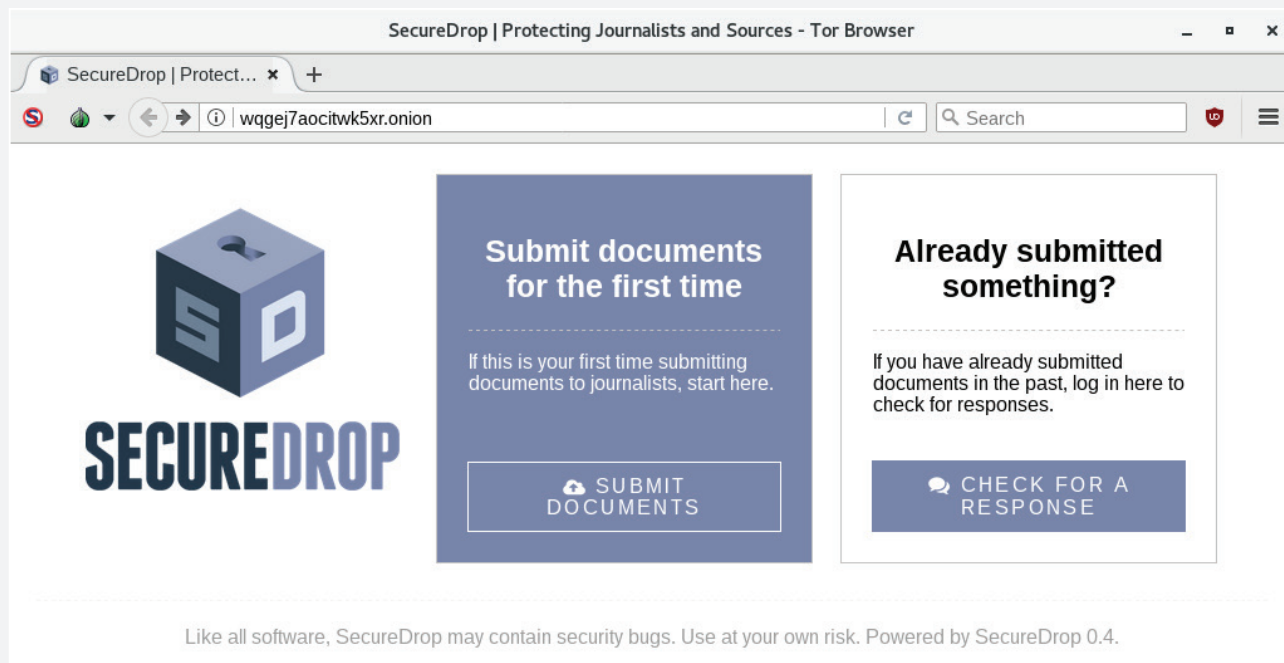


Pentru o securitate optimă, ultimul pas este ștergerea sesiunii prin **repornirea browserului Tor**. Puteți să închideți browserul în întregime sau să urmați notificarea: faceți clic pe sigla Tor din bara de instrumente, faceți clic pe **"New Identity"** (*Identitate nouă*) și apoi faceți clic pe **"Yes"** (*Da*) din caseta de dialog care apare pentru a confirma că doriți să reporniți browserul Tor:

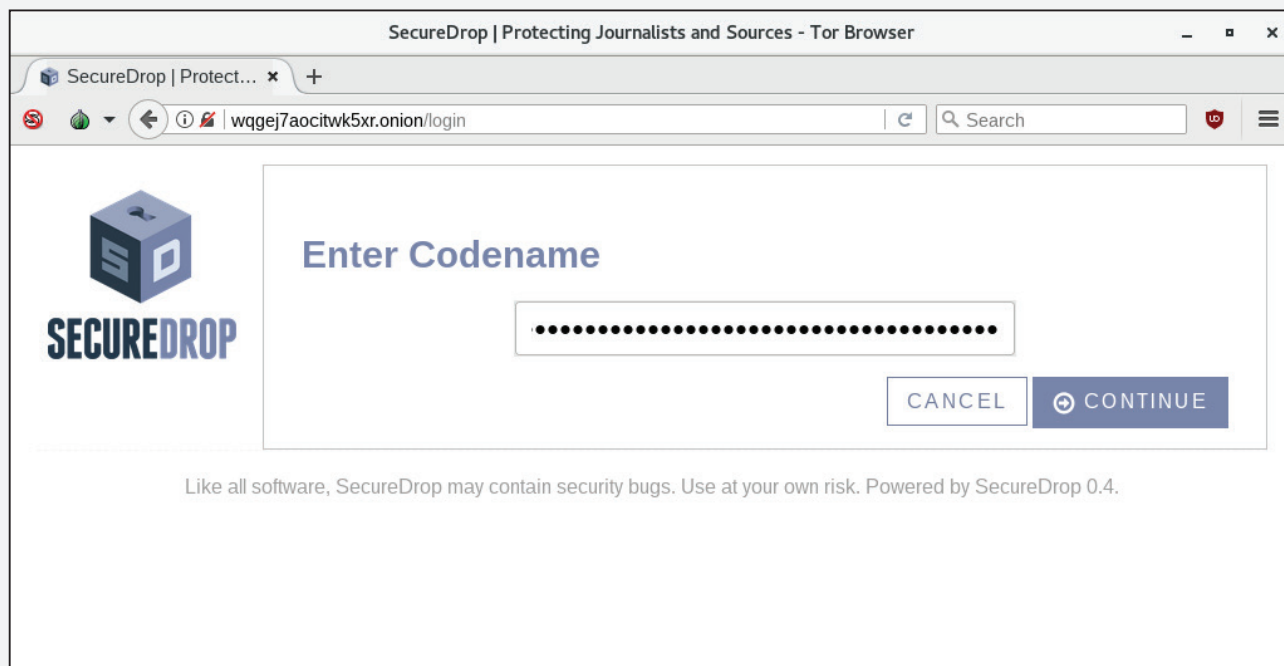


»» Continuă conversația după expedierea documentelor

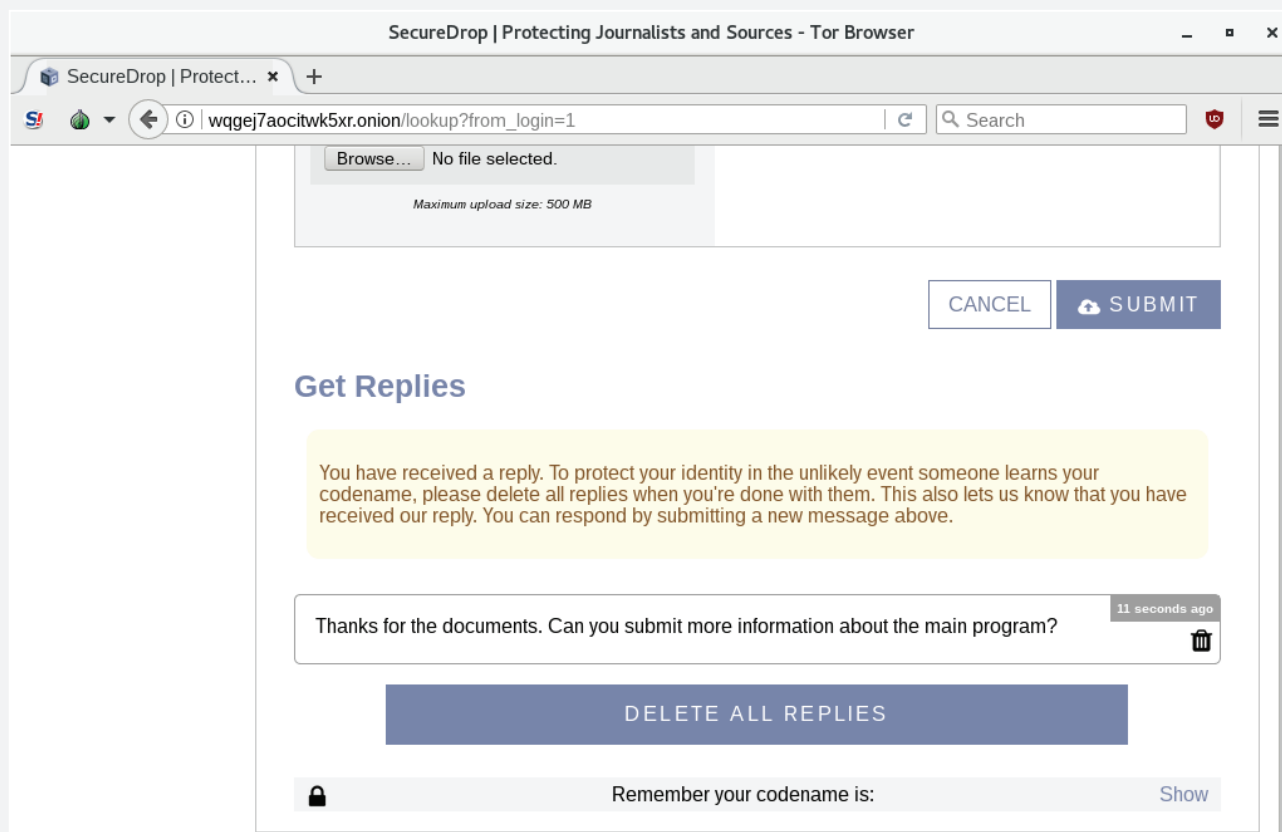
Dacă ați trimis deja un document și doriți să verificați răspunsurile, faceți clic pe butonul **"Check for a Response"** pe pagina de pornire SecureDrop a organizației media respective.



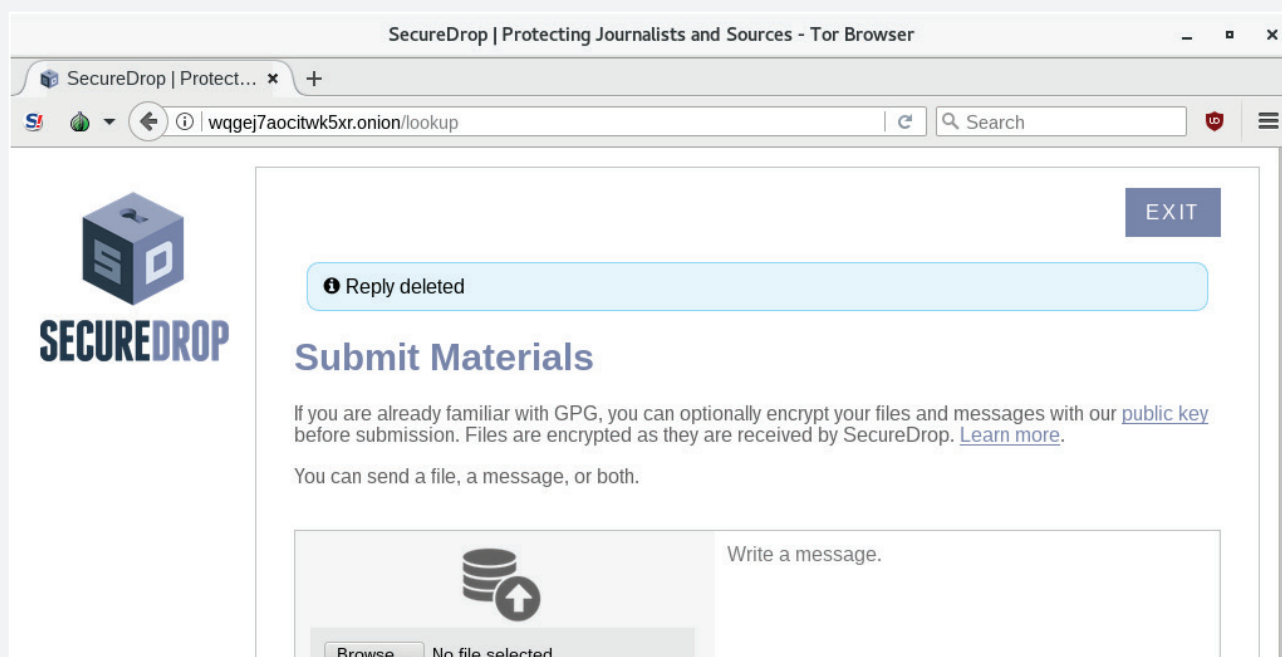
Următoarea pagină va cere **codul vostru unic secret**. Introduceți-l și faceți clic pe **"Continue"**.



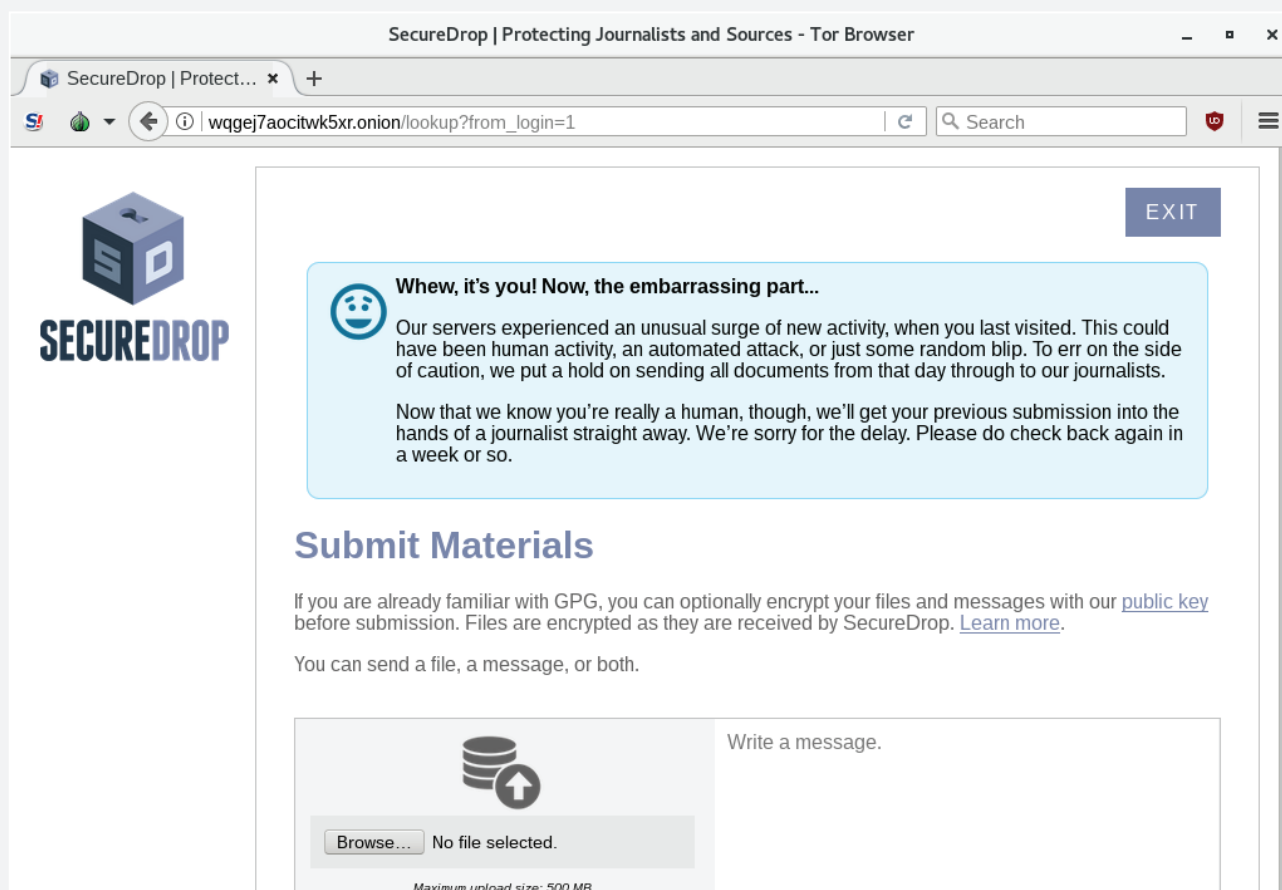
Dacă un jurnalist a răspuns, mesajul lui va apărea pe pagina următoare. Această pagină vă permite, de asemenea, să încărcați un alt document sau să mai expediați un mesaj jurnalistului. Înainte de a părăsi pagina, ar trebui **să ștergeți toate răspunsurile primite**. Astfel, dacă cineva va afla codul dvs. unic, chiar dacă e puțin probabil, aceasta măsură vă va păstra identitatea secretă, deoarece nimeni nu va putea vedea corespondența anterioară cu jurnaliștii.



După ce ștergeți conversația, **asigurați-vă că vedeți mesajul** de mai jos:



Dacă serverul se confruntă cu un număr mare de surse noi care se înregistrează simultan și este supraîncărcat cu expedieri, jurnalistul va semna mesajul dvs. la sfârșitul lor și **veți vedea mesajul de mai jos**. Din motive de securitate, **reporterii nu vă pot răspunde până când nu ați văzut acest mesaj**. Acest lucru se va întâmpla doar atunci când jurnalistul vă răspunde pentru prima dată. Răspunsurile ulterioare vor sări peste acest pas. Trebuie doar să faceți clic pe **"Refresh"** sau să vă conectați din nou pentru a vedea dacă jurnalistul v-a răspuns.



Repetăți acești pași pentru a continua comunicarea cu jurnalistul.