

# Task 1:

First we check how friend request works. We need to check the URL of GET request. Then we need to determine the guid of Samy. After we put the 1905006\_Task\_1.js in the script to Samy's profile. Then if any user visit Samy's profile a friend request will be sent automatically to Samy.

## 1.1. Checking how friend request work

The screenshot shows the Elgg For SEED Labs user profile for 'Alice'. The profile includes a header with navigation links (Blogs, Bookmarks, Files, Groups, Members, More -) and a search bar. Below the header is a profile picture of Alice and buttons for 'Remove friend' and 'Send a message'. The main content area shows a list of blogs and bookmarks. The bottom of the page features a network inspector showing a GET request to the URL: `http://www.seed-server.com/action/friends/add?friend=568_elgg_ts=17080891388_elgg_token=tpkkuw7Q1KdyHgPmRjPQLOA&jquery=2.2.3`. The response is a JSON object with status 200 OK. The response headers show: `Cache-Control: must-revalidate, no-cache, no-store, private`, `Connection: Keep-Alive`, `Content-Length: 388`, `Content-Type: application/json; charset=UTF-8`, and `Date: Fri, 16 Feb 2024 13:12:33 GMT`.

The screenshot shows the Elgg For SEED Labs user profile for 'Alice' after a successful friend request. The profile header and navigation links are the same. The main content area now shows a green notification message: 'You have successfully added Alice as a friend.' The bottom of the page features a network inspector showing a GET request to the URL: `http://www.seed-server.com/action/friends/add?friend=568_elgg_ts=17080891388_elgg_token=tpkkuw7Q1KdyHgPmRjPQLOA&jquery=2.2.3`. The response is a JSON object with status 200 OK. The response headers show: `Cache-Control: must-revalidate, no-cache, no-store, private`, `Connection: Keep-Alive`, `Content-Length: 388`, `Content-Type: application/json; charset=UTF-8`, and `Date: Fri, 16 Feb 2024 13:12:33 GMT`.

[illegible]

### 1.3. After visiting Samy's profile a request has been sent:

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search

Samy Remove friend Send a message

About me

Blogs Bookmarks Files Pages Wire post

Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Filter	Method	Domain	File	Initiator	Type	Transferred	Size	Time
182	POST	www.seed-server.com	edit	document	html	4.18 KB	18.45 KB	151 ms
183	GET	www.seed-server.com	samy	document	html	4.22 KB	18.45 KB	151 ms
184	GET	www.seed-server.com	5f1a7e.jpg	img	jpeg	cached	4.46 KB	3 ms
184	GET	www.seed-server.com	jquery.js	script	js	cached	0 B	3 ms
184	GET	www.seed-server.com	jquery.min.js	script	js	cached	0 B	3 ms
184	GET	www.seed-server.com	require_config.js	script	js	cached	789 B	8 ms
184	GET	www.seed-server.com	require.js	script	js	cached	0 B	7 ms
184	GET	www.seed-server.com	elgg.js	script	js	cached	0 B	7 ms
184	GET	www.seed-server.com	script.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	en.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	webpack-polyfill.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	formdata-polyfill.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	widgets.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	init.js	require.js!27 (script)	js	cached	370 B	0 ms
184	GET	www.seed-server.com	ready.js	require.js!27 (script)	js	cached	123 B	0 ms
184	GET	www.seed-server.com	lightbox.js	require.js!27 (script)	js	cached	0 B	11 ms

25 requests 55.23 KB / 8.40 KB transferred Finish: 4.05 s DOMContentLoaded: 2.54 s Load: 2.57 s

## Task2:

First we check how to upload profile data. For that we will upload the new profile data and check the POST URL and also check the payload. Then we will change the payload according to the user name and guid. Then we will write the script in Samy's profile. As a result when other users visit Samy's profile his/her profile information will automatically change.

### 2.1. Checking the POST request and payload:

Elgg For SEED Labs Blogs Bookmarks Files Groups Members More - Search

Samy Edit avatar Edit profile

Brief description  
1905006

Location  
Ultra Palta Location

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter URLs

Filter	Method	Domain	File	Initiator	Type	Transferred	Size	Time
182	POST	www.seed-server.com	edit	document	html	4.18 KB	18.45 KB	151 ms
183	GET	www.seed-server.com	samy	document	html	4.22 KB	18.45 KB	151 ms
184	GET	www.seed-server.com	5f1a7e.jpg	img	jpeg	cached	4.46 KB	3 ms
184	GET	www.seed-server.com	jquery.js	script	js	cached	0 B	3 ms
184	GET	www.seed-server.com	jquery.min.js	script	js	cached	0 B	3 ms
184	GET	www.seed-server.com	require_config.js	script	js	cached	789 B	8 ms
184	GET	www.seed-server.com	require.js	script	js	cached	0 B	7 ms
184	GET	www.seed-server.com	elgg.js	script	js	cached	0 B	7 ms
184	GET	www.seed-server.com	script.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	en.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	webpack-polyfill.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	formdata-polyfill.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	widgets.js	require.js!27 (script)	js	cached	0 B	0 ms
184	GET	www.seed-server.com	init.js	require.js!27 (script)	js	cached	370 B	0 ms
184	GET	www.seed-server.com	ready.js	require.js!27 (script)	js	cached	123 B	0 ms
184	GET	www.seed-server.com	lightbox.js	require.js!27 (script)	js	cached	0 B	11 ms

25 requests 55.23 KB / 8.40 KB transferred Finish: 4.05 s DOMContentLoaded: 2.54 s Load: 2.57 s

Samy

Edit avatar Edit profile



Brief description  
1905006  
Location  
Uita Palta Location

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	www.seed-server.com	edit	document	html	4.18 KB	18.45 KB
200	GET	www.seed-server.com	samy	document	html	4.22 KB	18.45 KB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.46 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	sprintf.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js!27 (scrip	js	cached	370 B
200	GET	www.seed-server.com	ready.js	require.js!27 (scrip	js	cached	123 B
200	GET	www.seed-server.com	lightbox.js	require.js!27 (scrip	js	cached	0 B

25 requests 55.23 KB / 8.40 KB transferred Finish: 4.05 s DOMContentLoaded: 2.54 s load: 2.57 s

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter Headers Cookies Request Response Timings

Filter Request Parameters

Request payload

1 Content-Disposition: form-data; name="\_\_\_elgg\_token"

2 Bn0Upccg6YrAB09oEIEAg

3 Content-Disposition: form-data; name="\_\_\_elgg\_ts"

4 1700809531

5 Content-Disposition: form-data; name="name"

6 Samy

7 Content-Disposition: form-data; name="description"

8 <p>Uita Palta About me</p>

9 Content-Disposition: form-data; name="accesslevel[description]"

10 1

11 Content-Disposition: form-data; name="location"

12 Uita Palta Location

13 Content-Disposition: form-data; name="accesslevel[location]"

14 1

Samy

Edit avatar Edit profile

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	www.seed-server.com	edit	document	html	4.18 KB	18.45 KB
200	GET	www.seed-server.com	samy	document	html	4.22 KB	18.45 KB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.46 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	sprintf.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	require.js!27 (scrip	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js!27 (scrip	js	cached	370 B
200	GET	www.seed-server.com	ready.js	require.js!27 (scrip	js	cached	123 B
200	GET	www.seed-server.com	lightbox.js	require.js!27 (scrip	js	cached	0 B

25 requests 55.23 KB / 8.40 KB transferred Finish: 4.05 s DOMContentLoaded: 2.54 s load: 2.57 s

Debugger Network Style Editor Performance Memory Storage Accessibility Application

Filter Headers Cookies Request Response Timings

Filter Request Parameters

Request payload

1 Content-Disposition: form-data; name="\_\_\_elgg\_token"

2 Bn0Upccg6YrAB09oEIEAg

3 Content-Disposition: form-data; name="\_\_\_elgg\_ts"

4 1700809531

5 Content-Disposition: form-data; name="name"

6 Samy

7 Content-Disposition: form-data; name="description"

8 <p>Uita Palta About me</p>

9 Content-Disposition: form-data; name="accesslevel[description]"

10 1

11 Content-Disposition: form-data; name="location"

12 Uita Palta Location



13 Content-Disposition: form-data; name="accesslevel[location]"

14 1

## 2.2 Before visiting Samy's profile:

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

**Alice**



Blogs

Bookmarks

Files


Pages

Wire post

## 2.3 After visiting Samy's profile:

**Alice**

Your profile was successfully saved



Blogs

Bookmarks

Files

Pages

Wire post

**Brief description**  
1905006

**Location**  
[Ulta Palta Location](#)

**Interests**  
 [Ulta Palta Interest](#)

**Skills**  
 [Ulta Palta Skill](#)

**Contact email**  
[UltaPaltaEmail@gmail.com](mailto:UltaPaltaEmail@gmail.com)

**Telephone**  
[Ulta Palta Telephone](#)

**Mobile phone**  
[Ulta Palta Mobile Phone](#)

**Website**  
<http://www.UltaPaltaWebsite.com>

**Twitter username**  
[Ulta Palta Twitter Username](#)

Debugger

Network

Style Editor

Performance

Memory

Storage

Accessibility

Application

## Task3:

First we check how to upload wire post. For that we will upload the wire post including Samy's profile link and check the POST URL and the payload. Then we will write the script in Samy's profile. As a result when other users visit Samy's profile a wire post will be automatically uploaded from his/he profile.

### 3.1 Checking the POST request and payload:

The screenshot shows a web browser window with the URL `www.seed-server.com/thewire/owner/samy`. The page displays a user profile for 'Samy' with a post that says 'To earn 12 USD/Hour(!), visit now [www.seed-server.com/profile/samy](\"http://www.seed-server.com/profile/samy\")'. Below the browser window, the Chrome DevTools Network tab is open, showing a list of requests. The first request is a POST to `http://www.seed-server.com/action/thewire/add`, which is highlighted. The right-hand pane shows the response headers for this request, including 'Status: 302 Found', 'Content-Type: text/html; charset=UTF-8', and 'Location: http://www.seed-server.com/thewire/owner/samy'.

Index	Method	Domain	File	Initiator	Type	Transferred	Size
01	POST	www.seed-server.com	add	document	html	4.69 KB	21.12 KB
02	GET	www.seed-server.com	samy	document	html	4.73 KB	21.12 KB
04	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
04	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
04	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
04	GET	www.seed-server.com	require.js	script	js	cached	0 B
04	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
04	GET	www.seed-server.com	spirit.js	require.js!27 (scri...	js	cached	0 B
04	GET	www.seed-server.com	en.js	require.js!27 (scri...	js	cached	0 B
04	GET	www.seed-server.com	weakmap-polyfill.js	require.js!27 (scri...	js	cached	0 B
04	GET	www.seed-server.com	formdata-polyfill.js	require.js!27 (scri...	js	cached	0 B
04	GET	www.seed-server.com	init.js	require.js!27 (scri...	js	cached	370 B
04	GET	www.seed-server.com	ready.js	require.js!27 (scri...	js	cached	123 B
04	GET	www.seed-server.com	lightbox.js	require.js!27 (scri...	js	cached	0 B
04	GET	www.seed-server.com	thewire.js	require.js!27 (scri...	js	cached	0 B
04	GET	www.seed-server.com	thewire.js	require.js!27 (scri...	js	cached	0 B

Filter Headers	Filter Cookies	Filter Request	Filter Response	Filter Timings
POST	http://www.seed-server.com/action/thewire/add			
Status	302 Found			
Version	HTTP/1.1			
Transferred	4.69 KB (21.12 KB size)			
Referer Policy	no-referrer-when-downgrade			
Response Headers (402 B)				
Cache-Control	must-revalidate, no-cache, no-store, private			
Connection	Keep-Alive			
Content-Length	426			
Content-Type	text/html; charset=UTF-8			
Date	Fri, 16 Feb 2024 13:29:39 GMT			
Expires	Thu, 19 Nov 1981 08:52:00 GMT			
Keep-Alive	timeout=5, max=100			
Location	http://www.seed-server.com/thewire/owner/samy			
Pragma	no-cache			
Server	Apache/2.4.41 (Ubuntu)			
Vary	User-Agent			

Application

Size 21.12 KB

Headers Cookies **Request** Response Timings

Filter Request Parameters

Request payload

```
1 -----40431044812712565118709283409
2 Content-Disposition: form-data; name="__elgg_token"
3
4 m8F1QadUXNHXLdwjqncs5w
5 -----40431044812712565118709283409
6 Content-Disposition: form-data; name="__elgg_ts"
7
8 1708090150
9 -----40431044812712565118709283409
10 Content-Disposition: form-data; name="body"
11
12 To earn 12 USD/Hour(!), visit now
13 www.seed-server.com/profile/samy
14 -----40431044812712565118709283409--
15
```

### 3.2. Before visiting Samy's profile:

www.seed-server.com/thewire/owner/alice

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

Alice > Wire posts

## Alice's wire posts

All **Mine** Friends

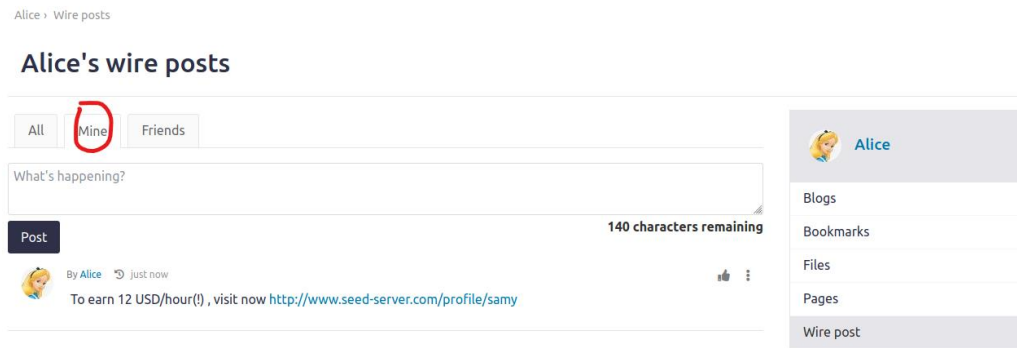
What's happening?

Post 140 characters remaining

Alice

- Blogs
- Bookmarks
- Files
- Pages
- Wire post

### 3.3. After visiting Samy's profile:



## Task4:



It's basically the concatenation of the previous three tasks. Here we have to do some extra work. That is we have to put the worm code in the description. And also in the wire post we will put the user's profile id link instead of Samy's profile id link. Here if one user like Alice visit Samy's profile then she will be affected. Again if other user like Bobby visit Alice's profile he will be affected. As a result it is self propagated.



#### 4.1.1. Before visiting Samy's profile:

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



**Alice** Edit avatar Edit profile



[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

#### 4.1.2 After visiting Samy's profile:

**Alice** Edit avatar Edit profile



[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

**Brief description**  
1905006

**Location**  
[Ulta Palta Location](#)

**Interests**  
 [Ulta Palta Interest](#)

**Skills**  
 [Ulta Palta Skill](#)

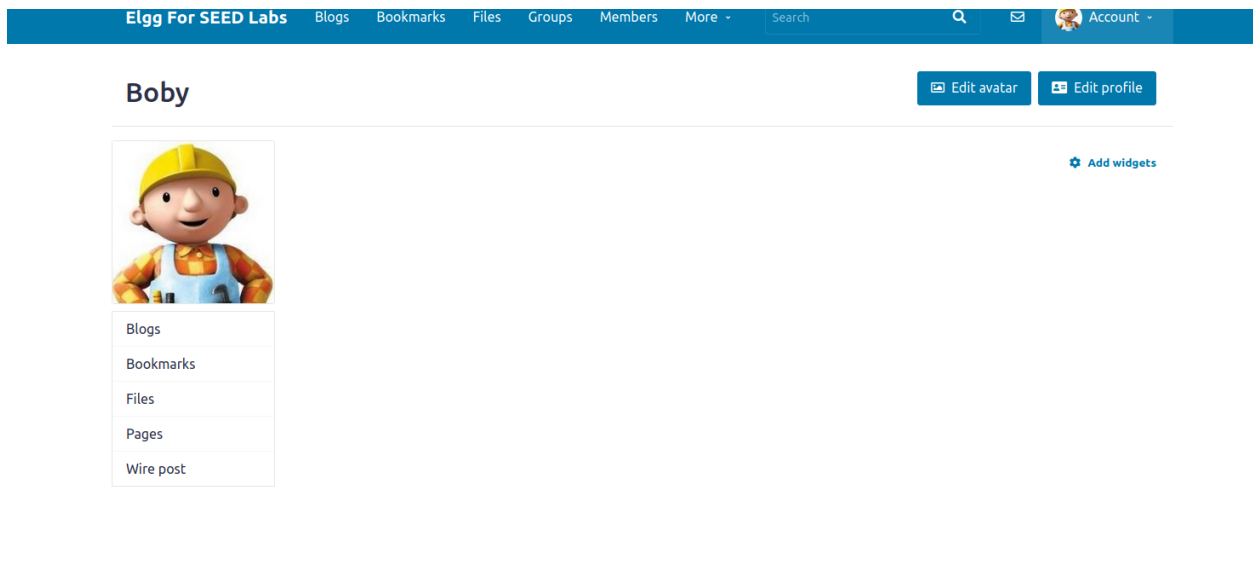
**Contact email**  
[UltaPaltaEmail@gmail.com](mailto:UltaPaltaEmail@gmail.com)

**Telephone**  
[Ulta Palta Telephone](#)

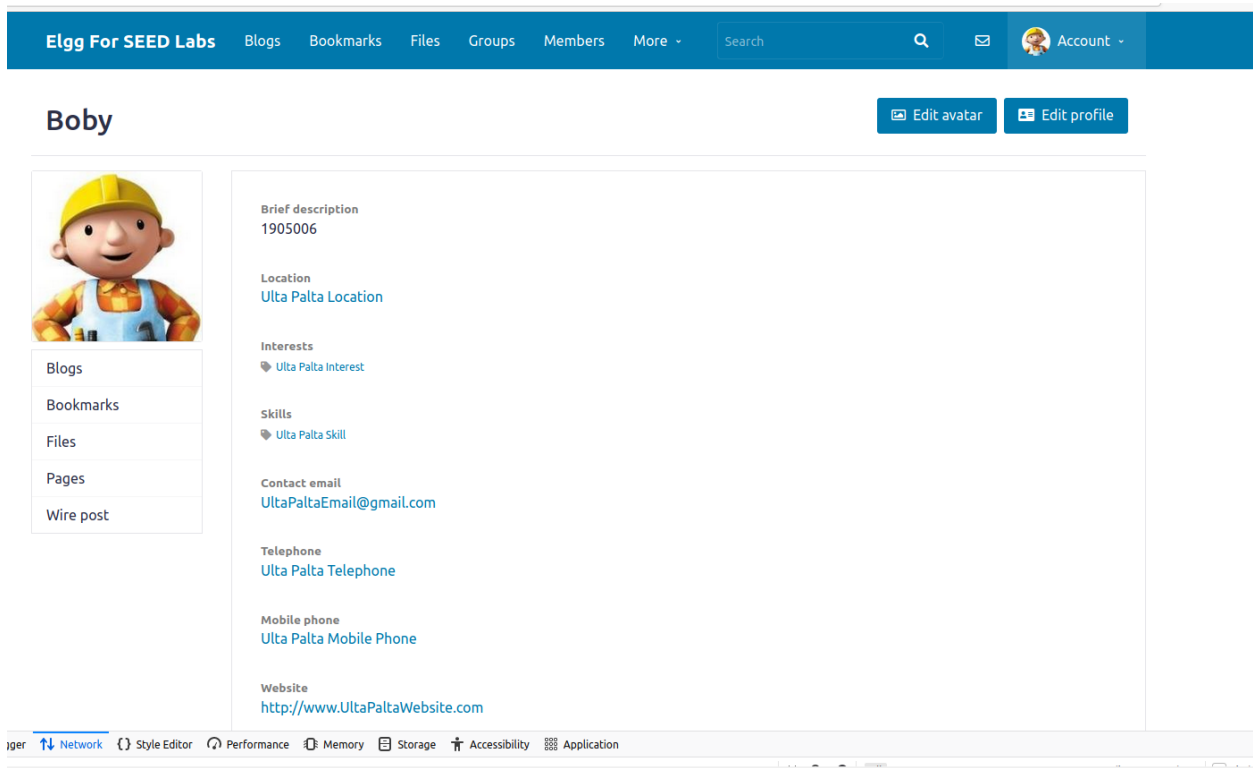
**Mobile phone**  
[Ulta Palta Mobile Phone](#)

**Website**  
<http://www.UltaPaltaWebsite.com>

#### 4.2.1. Before visiting Alice's profile:



#### 4.2.2. After visiting Alice's profile:





#### 4.3.2. After visiting Bobby's profile:

Elgg For SEED Labs


BlogsBookmarksFilesGroupsMembersMore

Search

Account

Charlie

Edit avatarEdit profile



Blogs

Bookmarks

Files

Pages

Wire post

Brief description

1905006

Location

Ulta Palta Location

Interests

Ulta Palta Interest

Skills

Ulta Palta Skill

Contact email

UltaPaltaEmail@gmail.com

Telephone

Ulta Palta Telephone

Mobile phone

Ulta Palta Mobile Phone

Website

http://www.UltaPaltaWebsite.com


Charlie > Wire posts

Charlie's wire posts



AllMineFriends


What's happening?

Post140 characters remaining



By Charlie just now


To earn 12 USD/hour(!) , visit now <http://www.seed-server.com/profile/Charlie>





By Charlie just now


To earn 12 USD/hour(!) , visit now <http://www.seed-server.com/profile/Charlie>



By Charlie just now

To earn 12 USD/hour(!) , visit now <http://www.seed-server.com/profile/Charlie>



Charlie

Blogs

Bookmarks

Files

Pages

Wire post