

Exploiting Gadu-Gadu

- \$ whoami

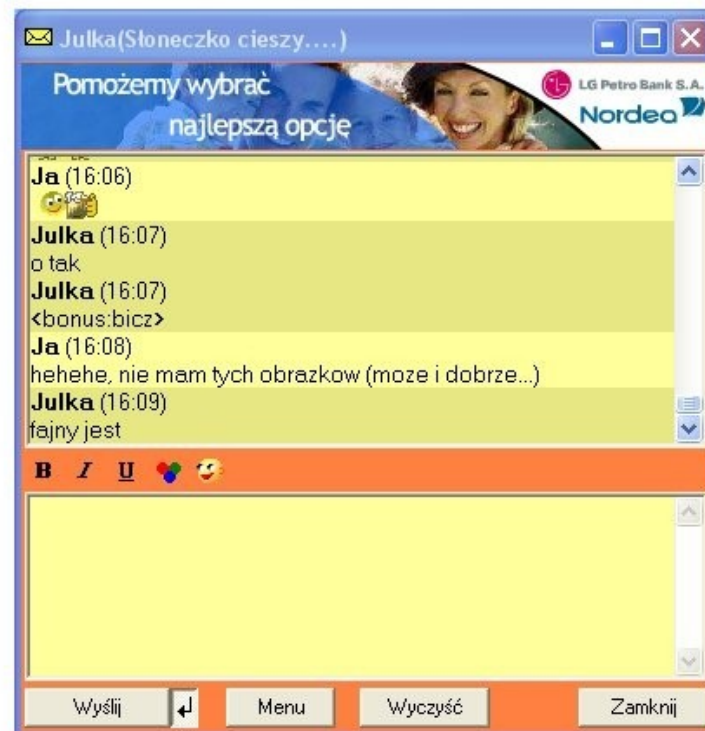


What's Gadu-Gadu?

- Feature rich Instant Messenger
- Most popular IM service in Poland
- 15M registered accounts
- 300M messages / day
- Adware
- Market value ~ \$150M

To make long story short...

- In 2005 people all over the world were using Skype, meanwhile in Poland...



Result? Bloat!



Karolina GG
Numer GG: 801

35587
otrzymanych upominków

Podaruj



Club

Nowa stacja w **OPENFM**

Impreza z selekcją




sluchaj »

Napisz **Zadzwoń** **Wideo** **Zagraj** **Więcej**

GG 10 - x (35799909)



Gadu-Gadu Kontakty Sklep Moje Usługi


KONKURS MAGNUM
WYGRAJ WYCIECZKĘ W DOWOLNE
MIEJSCE NA ŚWIECIE


   profil


Tutaj wpisz swój opis


Kontakty Ostatnie


Szukaj w kontaktach  **dodaj** 


► **Moje kontakty** 0/2 


▼ **Pomocnicy** 5/5 


 **Blip.pl**
Napisz, co teraz robisz


 **EzoBot**
Sprawdź horoskop, poznaj znaczenie imienia, odkryj tajemnice snów **(142)**

 **GaduAIR**
2 grosze za SMS! <http://gaduaire.pl/oferta>


 **Infobot**
Ciagle o czymś zapominasz? Zobacz www.infobot.pl/alarm


 **Karolina GG** profil

► **Ignorowani** 0/0 

 **więcej faktów**

- W pociągach PKP Intercity będzie darmowy Internet
- Statystyczna para kłóci się 7 razy dziennie

11° 

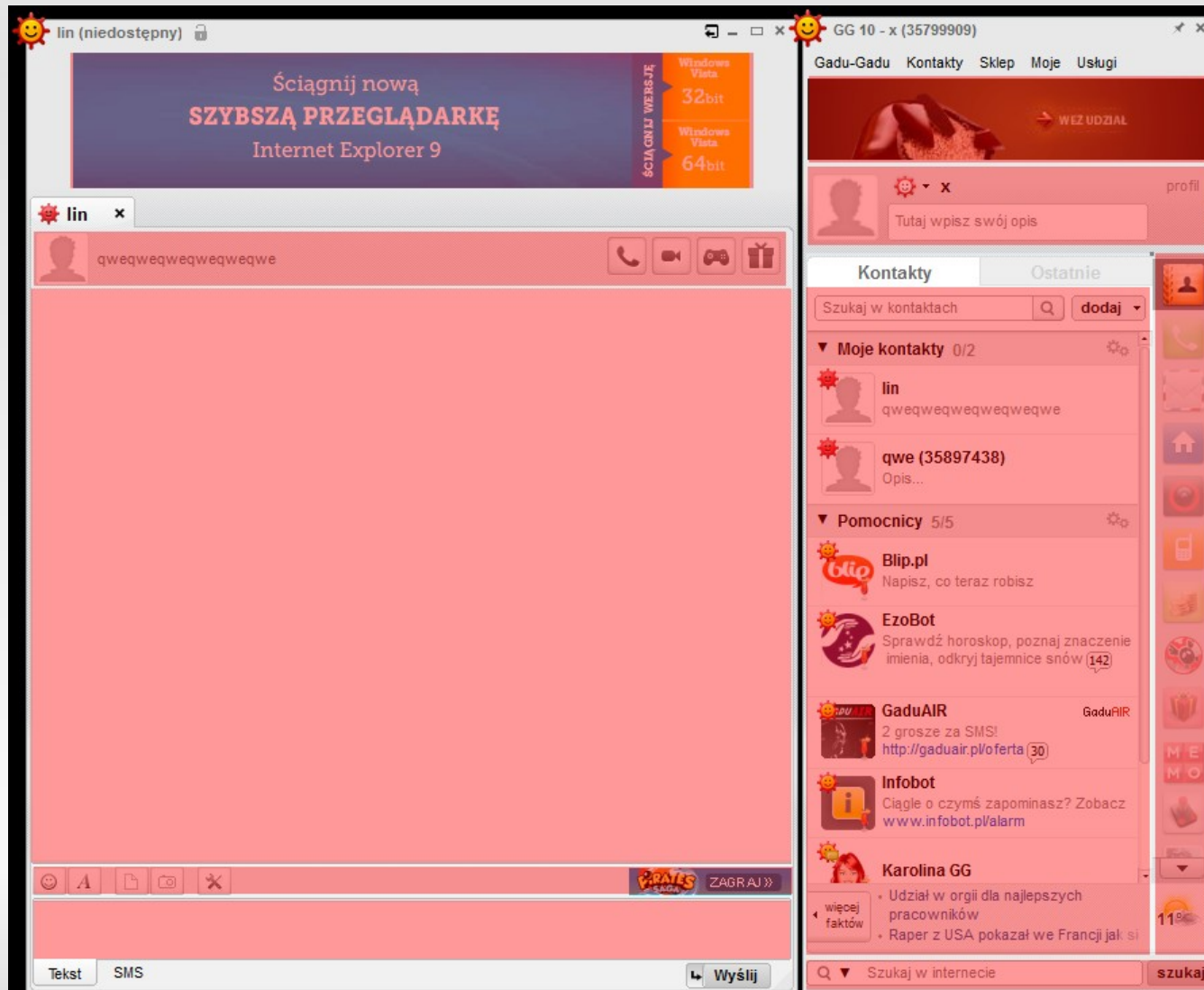
 Szukaj w internecie **szukaj**

Design

- Qt 4.7
- WebKit
 - Used for (flash) ads and User Interface
 - Integrated HTML content [news feeds]
- other software [random order]:
 - curl, openssl, libxml2, gstreamer, sqlite, zlib, iconv, glib, pjsip, ...
- Still windows only

More on UI design

- User Interface is really a set of web pages



UI implementation

- It's HTML/CSS and JavaScript
 - stored in templates or loaded during run-time
- Communication with core app

- Exposing C++ objects to JavaScript

```
webframe->addToJavaScriptWindowObject("someName", myObject);
```

- Internal protocols

```
gginternal://  
gginternalsendsms://  
open-openfm:  
oauth://  
gginternalnaglos://  
gginternalfileaccept://  
gginternalfiledeny://  
...
```

Hunting for bugs

- We can try to fuzz the protocol or ...

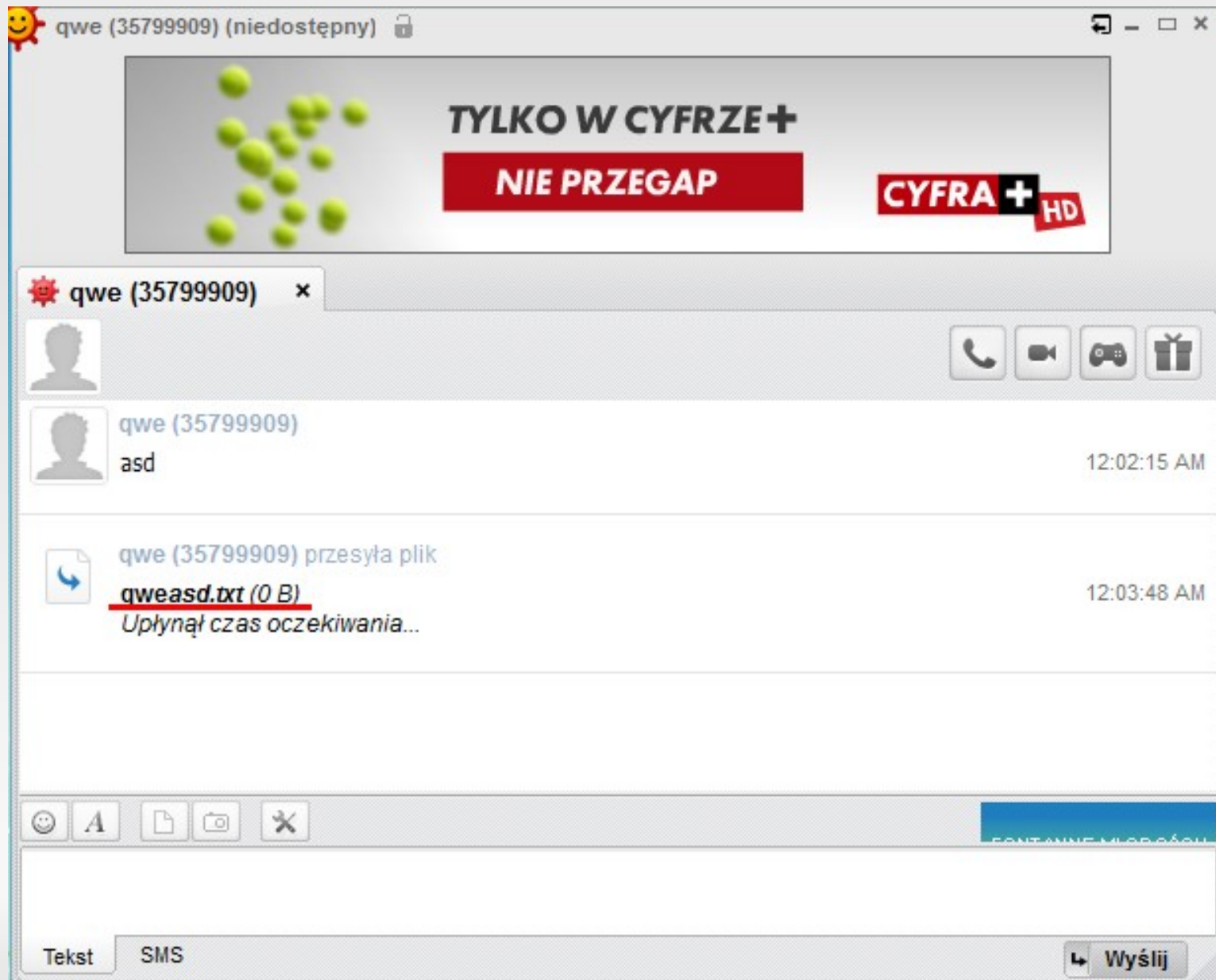
Hunting for bugs

- We can try to fuzz the protocol or ...
- Or find a XSS ...
- Attack vectors?
 - Malformed links
 - User status messages
 - Chat window
 - Ads
 - ... many, many more

Chit Chat

- Chat window
- File transfer dialog
- Improper filename handling
- 256 chars of HTML code
- Qt uses UNIX paths even on Windows
- No /
- Thus, no `<script>` tag

Sending <i> file



Executing JS

- How to execute JS code without `<script>` tag
 - Using an event handler
- Without user interaction
 - `<input onfocus='...' autofocus>`
- To load external script?
 - Dynamically create script node
 - `eval(unescape('...'))`

Taking over the control

- No window object in Chat Window
- Use gg internal protocols
 - `xxx`
 - Is it really a protocol?
 - `QwebPage::LinkDelegationPolicy`
- Triggering a click
 - `HTMLEvents`
- Spawning process

Here's the plan

- Inject HTML and execute JS
- Load external script
- Hide all file requests and transfers
- Accept all transfers
- ShellExecute uploaded stuff

Demo

That's it!

- Questions?
- Comments?

Kacper Szczesniak
kacper3.14@gmail.com
+48 507 049 572

New Gadu-Gadu

- MIH bought Gadu-Gadu in 2008
- New owner decided to rewrite it from scratch
- Goals:
 - More Ads
 - Modern internal design
 - Nice look&feel
 - Cool features: text-chat, voip, video, games, email, VMNO, integration with social media, ip radio, news portal etc
 - Empowered marketing features
 - Customizable UI
 - Enhanced protocol

To make long story short...

- Started in 2000 by Łukasz Foltyn
- Who stated that "GG is very secure because it does not leave any TCP/IP ports open" ...
- It was so cool that the first release was already named version 3.0
- Idea based on ICQ
- Numerical UID
- Proprietary, binary protocol
- C2S model, no fancy P2P
- Direct connections used only for file/voice transfer
- Got extremely popular in next few years