freeLove

As you might know it is not so easy to find a girl when you stay behind your PC all day (including the nights). But at least here in Germany there is a solution to that problem.

It is called “dating sites”. That is a webpage where you can enter details about yourself and view the profiles of others who you might like to date. Some popular sites are: www.iLove.de www.neu.de www.meetic.de

This article is about exploiting the one with the most similar name to the headline.

„Love is like software - it is better when it is free“

One day we were driving in our car down some dark and cloudy road passing depressive thoughts. We somehow came up with the subject of these dating sites. Tim (who is the more social/communicative type) had already tried something like that (Jan would be rather too shy for that kind of thing).

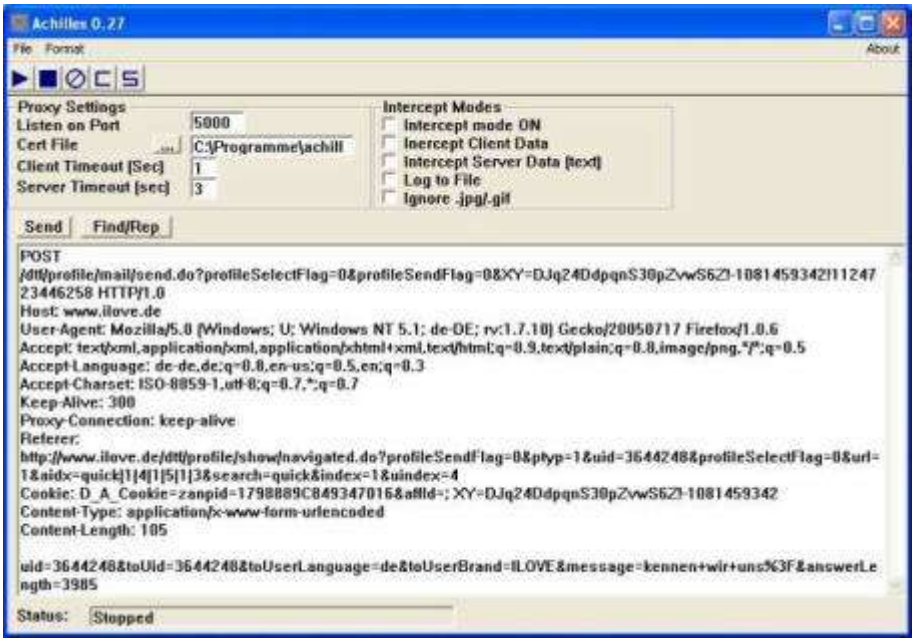
The main thing that had pissed Tim off was that he had to pay for talking to other people (girls) on that site. The point is that these services let you pay a certain fee per month so you can use features like sending emails to other users which is obviously the only thing you use that page.

Jan however knew from his sister that it is possible for girls to send messages to guys (not girls) for free. Any way to mess with that?

Setting up the test environment

To do a replay of that situation we created a guy and a girl on a popular dating site. The marvellous girl was named “himbaereis“ and the stunning guy had the nick “mikesCoolMail”. Maybe you come across those two (be warned: they will not date YOU).

To see what is going on over the line we used some tools like the good old ethereal and the pretty unstable but useful Achilles. Achilles is a proxy that can open up even ssl-connections and displays the information sent in requests and responses.



Achilles displaying the http-request sent to transmit a message

As usual for these meetings we also had bunches of coke and espresso ready to help us out.

Sniffing the glue that holds the Love together

First we had to find out what was going on when sending a message to another user. In the first place we started out with the girl's account sending messages to other guys. Since it was in the late evening many people were online and saw us visiting their profiles. We tried to keep the traffic low and not to disturb too many other legitimate users.

When we kind of found out that the only thing distinguishing the recipient was his uid we tried to mess with that. Sending mails to ourselves would be kind of useless. So we picked out a good looking girl that we wanted to date. Finding out the uid is pretty simple since it is part of the link to the user's profile.

We told that girl to send us a messages back if this thing worked out. She probably had no interest in a girl-girl relationship.

The uid is easily captured from the url of the profile

Works for girls but not for us

After some playing around with the request data we finally figured out how to send messages to girls. The way we did it was that we logged in as himbaereis and started writing a message to a guy. When the message was submitted we intercepted it using Achilles and replaced the recipients uid with the girl's one who we wanted to date.

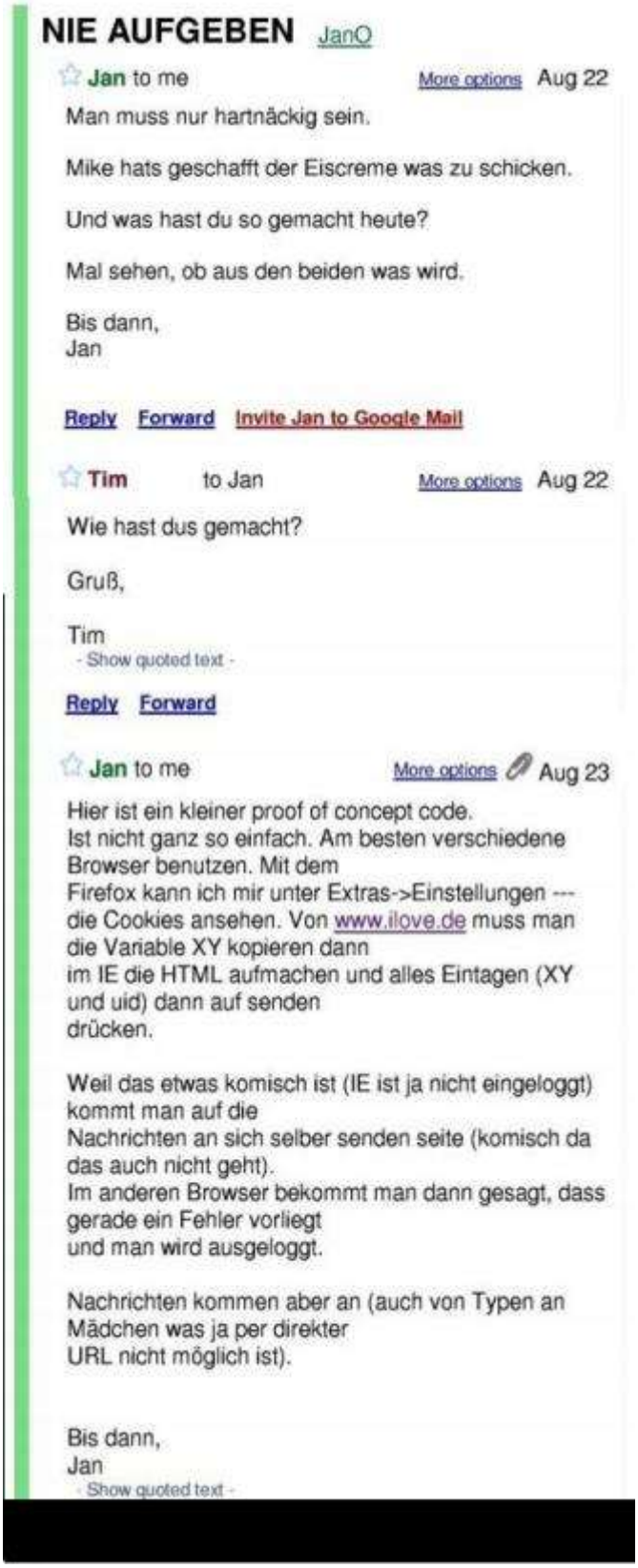
We immediately started writing a letter of complaint to team of iLove.

When suddenly Tim remembered that we in fact were boys not girls and so it was in question if we could even do the same attack while being logged in as guys.

This was the birth of "mikesCoolMail" (introduced above). We tried to just send any message to someone but had to realize that while girls could write boys, boys were not able to send any messages.

At that point (around 3 am) our world collapsed. Disappointed we crawled into our beds and cried ourselves to sleep. Could that be the end of our genius work?

No retreat, no surrender



NIE AUFGEBEN JanO

Jan to me More options Aug 22

Man muss nur hartnäckig sein.

Mike hats geschafft der Eiscreme was zu schicken.

Und was hast du so gemacht heute?

Mal sehen, ob aus den beiden was wird.

Bis dann,
Jan

Reply **Forward** **Invite Jan to Google Mail**

Tim to Jan More options Aug 22

Wie hast dus gemacht?

Gruß,

Tim
- Show quoted text -

Reply **Forward**

Jan to me More options Aug 23

Hier ist ein kleiner proof of concept code.
Ist nicht ganz so einfach. Am besten verschiedene Browser benutzen. Mit dem
Firefox kann ich mir unter Extras->Einstellungen --- die Cookies ansehen. Von www.ilove.de muss man die Variable XY kopieren dann
im IE die HTML aufmachen und alles Eintagen (XY und uid) dann auf senden
drücken.

Weil das etwas komisch ist (IE ist ja nicht eingeloggt) kommt man auf die
Nachrichten an sich selber senden seite (komisch da das auch nicht geht).
Im anderen Browser bekommt man dann gesagt, dass gerade ein Fehler vorliegt
und man wird ausgeloggt.

Nachrichten kommen aber an (auch von Typen an Mädchen was ja per direkter
URL nicht möglich ist).

Bis dann,
Jan
- Show quoted text -

An important conversation the next days

When Tim woke up the next day (about late afternoon…), he found a mail in his box, Jan had written. He finally found a way to have Mike send a mail to himbaereis. Victory was ours.

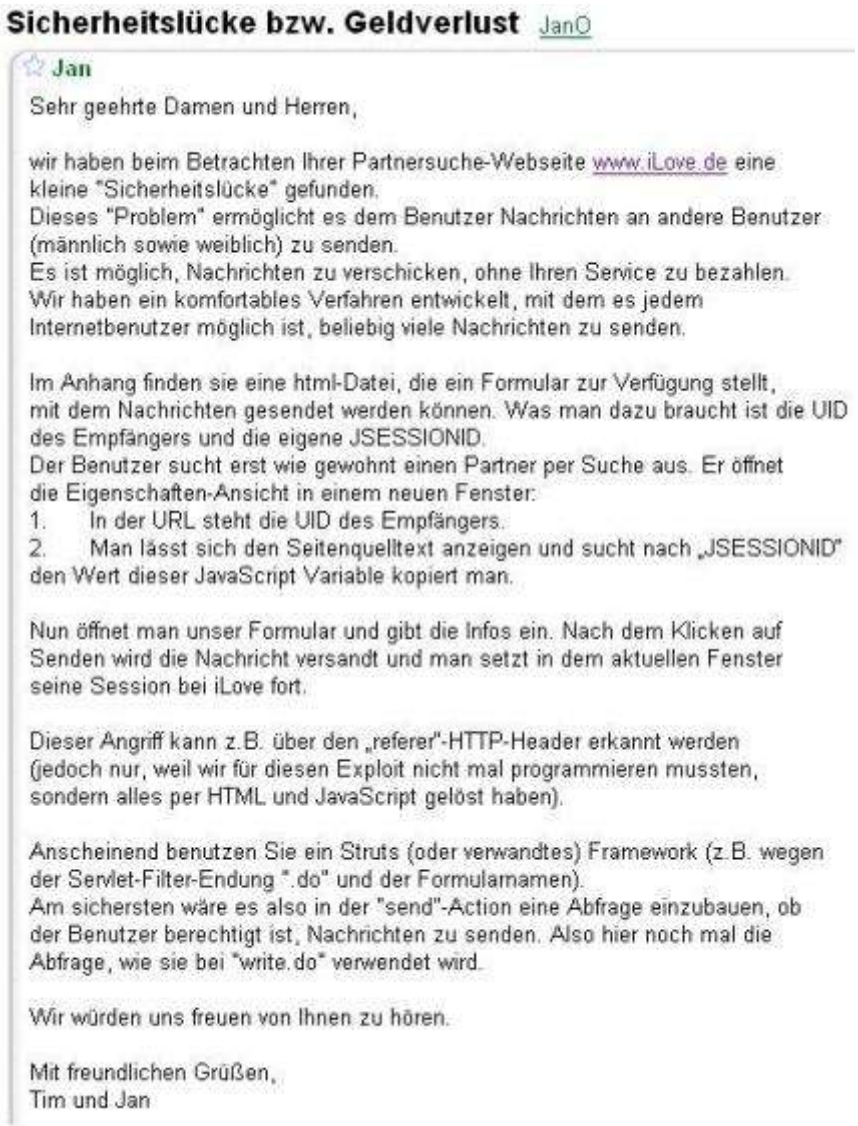
When we first tried to send a message as a boy, we could not get past the “pay for this”-screen. It seemed that guys cannot do anything in the system. Jans idea was to make our own user-form which we could use to compile our messages. After that, our old trick with faked uids worked again.

To make this work, we just needed a little old-fashioned HTML and JavaScript knowledge, to make our messages look like they were sent from a valid user-account.

You can find the source code here.

Our love got rejected

Being the nice guys we are, we wrote an email to ilove.de



Sicherheitslücke bzw. Geldverlust JanO

Jan

Sehr geehrte Damen und Herren,

wir haben beim Betrachten Ihrer Partnersuche-Webseite www.iLove.de eine kleine "Sicherheitslücke" gefunden.
Dieses "Problem" ermöglicht es dem Benutzer Nachrichten an andere Benutzer (männlich sowie weiblich) zu senden.
Es ist möglich, Nachrichten zu verschicken, ohne Ihren Service zu bezahlen.
Wir haben ein komfortables Verfahren entwickelt, mit dem es jedem Internetbenutzer möglich ist, beliebig viele Nachrichten zu senden.

Im Anhang finden sie eine html-Datei, die ein Formular zur Verfügung stellt, mit dem Nachrichten gesendet werden können. Was man dazu braucht ist die UID des Empfängers und die eigene JSESSIONID.
Der Benutzer sucht erst wie gewohnt einen Partner per Suche aus. Er öffnet die Eigenschaften-Ansicht in einem neuen Fenster:
1. In der URL steht die UID des Empfängers.
2. Man lässt sich den Seitenquelltext anzeigen und sucht nach „JSESSIONID" den Wert dieser JavaScript Variable kopiert man.

Nun öffnet man unser Formular und gibt die Infos ein. Nach dem Klicken auf Senden wird die Nachricht versandt und man setzt in dem aktuellen Fenster seine Session bei iLove fort.

Dieser Angriff kann z.B. über den „referer"-HTTP-Header erkannt werden (jedoch nur, weil wir für diesen Exploit nicht mal programmieren mussten, sondern alles per HTML und JavaScript gelöst haben).

Anscheinend benutzen Sie ein Struts (oder verwandtes) Framework (z.B. wegen der Servlet-Filter-Endung ".do" und der Formularnamen).
Am sichersten wäre es also in der "send"-Action eine Abfrage einzubauen, ob der Benutzer berechtigt ist, Nachrichten zu senden. Also hier noch mal die Abfrage, wie sie bei "write.do" verwendet wird.

Wir würden uns freuen von Ihnen zu hören.

Mit freundlichen Grüßen,
Tim und Jan

Our letter to the people in charge at iLove.de

The letter mainly tells them the things we just told you in the above text plus a step by step description, how to use the proof of concept.

We never heard from them. At least THEY should know, how important communication is in a relationship.