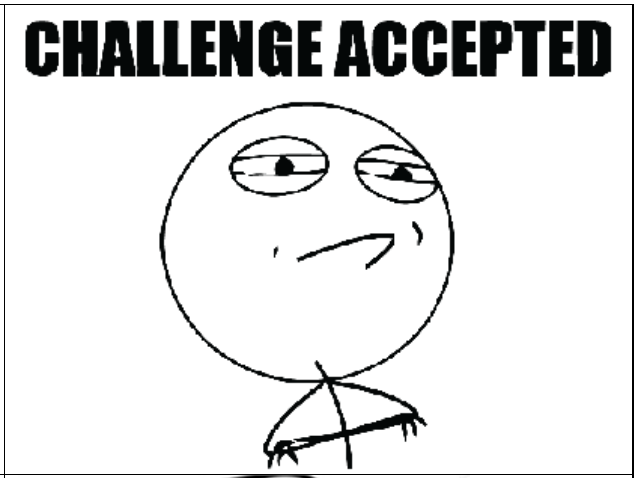
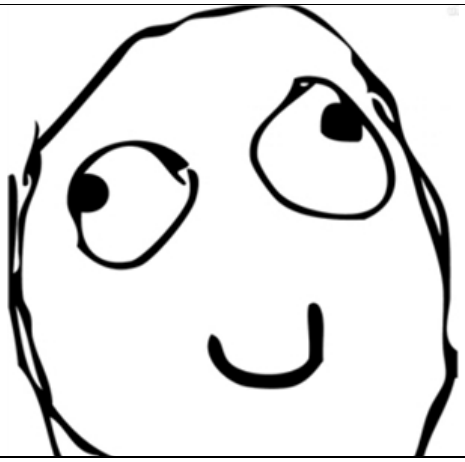
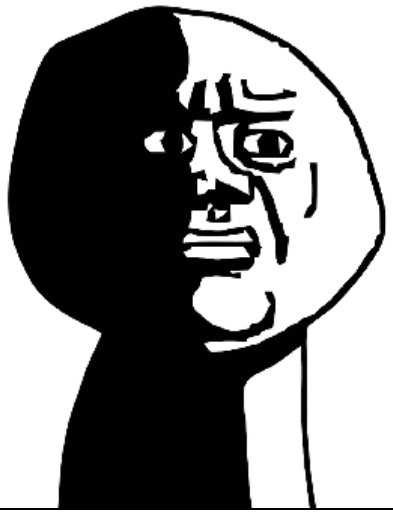
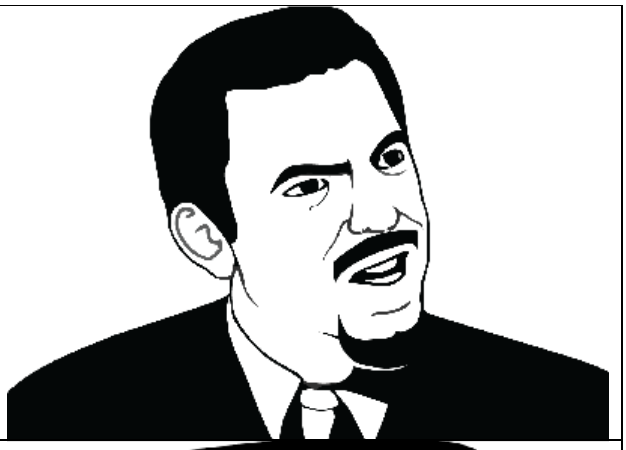
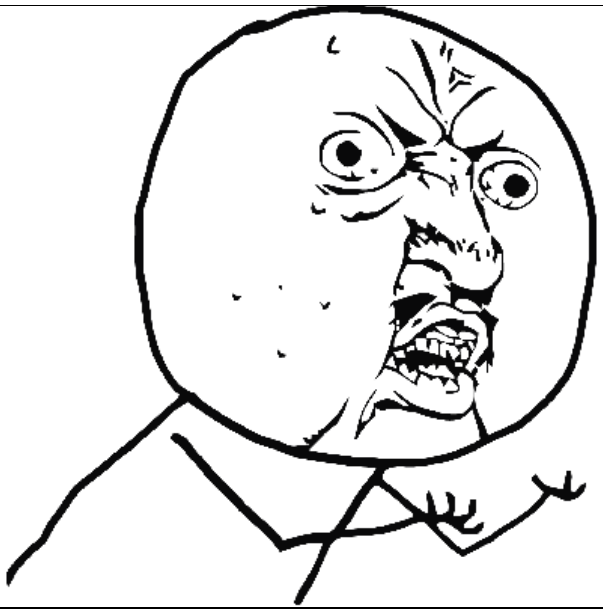
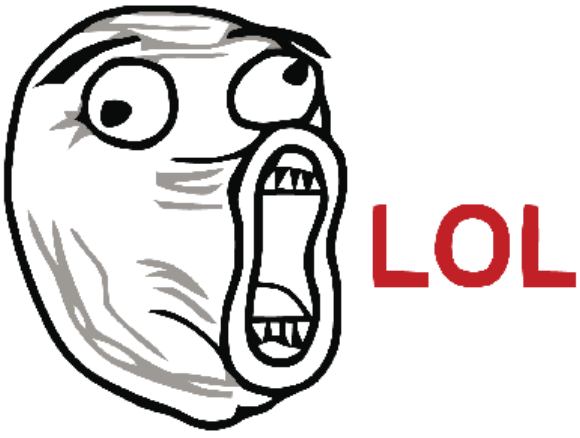
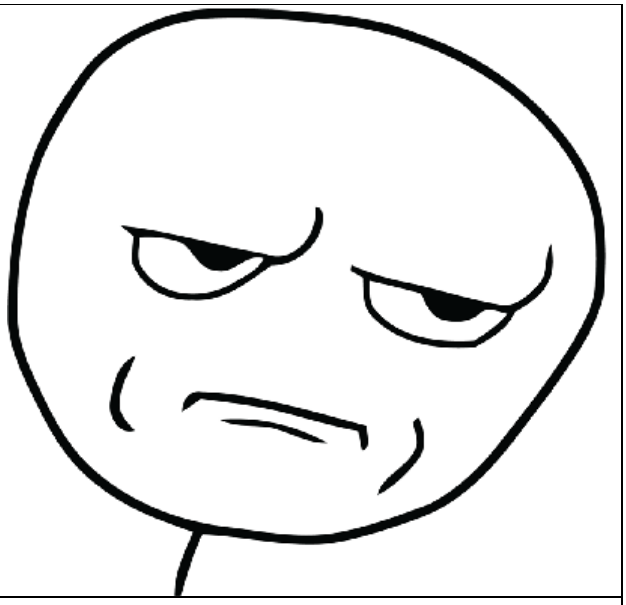
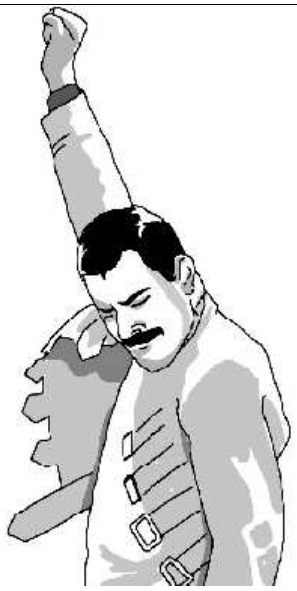
| | |
|---|---|
| Le me reading some usual stuff at work, when suddenly ...<br><br>SANS Holiday Challenge 2012 !!!<br><br>Let's go with it ! |  |
| Hmmm, Snowmiser, Heatmiser, the storyline looks funny, it shouldn't be hard I guess. Let's start with this Snowmiser guy... |  |
| LOL, that's gonna be a piece of cake! This guys just use static URLs. Let's google for a piece of it... Here we are, just like suspected, there are some on Pastebin. But hmmm, why doesn't any of them work?! Bruteforcing? This is GUID, it's gonna take sun's lifetime. No, it can't be that hard ... I haven't even started yet ... |  |

| | |
|---|---|
| No, let's take a break from cracking URLs and read one of these twitters...<br><br>Hmmm, they mention GUIDs indeed and... wait, there is something on this picture...<br>... now way, it was so easy all that time? seriously ?<br><br>So here I am in Snowmiser's Zone 1. The flag is `38bef0b61ba8edda377b626fe6708bfa` |  |
| Hmmm, to get to zone 2 I need to ... "analyze the images"?! Not again! I've already spent too much time on Twitter.<br>... maybe, let's try this dump of android smartphone instead. Let's just search it looking for "zone-" and ... Bingo! Zone 3 in browser's cache! And Zone 3 has a valid URL to Zone 2! Nice shot!<br>And the flags are<br>Zone 2:<br>`b8231c2bac801b54f732cfbdcd7e47b7`<br>and Zone 3:<br>`08ba610172aade5d1c8ea738013a2e99` |  |
| ... but later on, I don't feel comfortable about this shortcut directly to Zone 3. Let's go back to those images again.<br>There isn't any additional URL on this picture that's what I'm sure about. Maybe that's this status image on the website? I don't see anything suspicious here. ... but wait! After I press the "Disable" button there's JPG instead of PNG. Why so? Hey, you can have an EXIF in JPG, let's check it! There is EXIF indeed and ... IceIceBaby! That has to be some sort of key... Of course! Steganography! Let's just feed Steghide with it and: TADA! Zone 2 is legally mine. |  |

| | |
|---|---|
| Ok then, we're on again!<br>URL to Zone 4 is encrypted.<br>But!<br>... there's an old URL in both encrypted and plaintext form. Let's just extract a key by XORing them together (in hex) and then XOR this key with the ciphertext and ...<br>... WHY U USE ONE TIME PAD MORE THAN ONCE ???!!! (that's a very bad idea)<br>And I'm in Zone 4:<br>`de32b158f102a60aba7de3ee8d5d265a` |  |
| I'm almost at Zone 5. What I need is just ... one time password...<br>Hmmm, if I can only find out how they are generated... Twitts may be helpful again as one of the guys mentions some SVN leakage. That may be extremely useful... And that's it! SVN database file is mine! Let's just parse it to see where index.php source is and...<br>Bingo! OTP are generated just by hashing time with salt. Let's create one... Oh, we need to use server's local time I suppose, add some salt and...<br>Voilà – Zone 5!<br>`3ab1c5fa327343721bc798f116be8dc6` |  |
| Snowmiser's owned. Time for his brother. Let's take a look: they mention something about search engines. I'd laugh if I hadn't seen such cases so many time with so many "secured" sites before. And that's it, quick googling and here we are in Heatmiser's Zone 1:<br>`d8c94233daef256c42bb95bd61382e02` |  |

| | |
|---|---|
| URL to Zone 2 has been removed ... and left commented in the page's source...<br><br>Zone 2:<br>ef963731de7e886226fe4a6a6c2971f1 |  |
| So, no clue how to get next URL ... They mention something about mail, let's see if this host serves SMTP. ... nope, it doesn't. Then Twitters again ? Going through again and again... still without any clue. ...hey wait! what kind of "transparent terminal" do you mean? let's set a contrast of this screenshot to maximum value and ...<br>Zone 3 !<br>0d524fb8d8f9f88eb9da5b286661a824 |  |
| Hmmm, link to Zone 4 doesn't contain any login form nor anything like that. Maybe cookie ? Nope, there isn't any. But wait! This response looks pretty big. Let's look inside. LOL, redirection without exit() gave me full source of Zone 4 including link to Zone 5.<br>Zone 4:<br>e3ae414e6d428c3b0c7cff03783e305f |  |

| | |
|---|---|
| And the very last one. No login form again, but here's cookie. Let's see: this string looks like some hashed value. In fact it is! Quick checking in some rainbow tables and that's MD5 for "1001". I guess that's a default user ID for a user without any access. It's hashed without any salt nor any additional value – what I need to do the is just find a MD5 for a user with access. Unsuccessfully trying some common values ... Some clues on Twitter... Nope, sorry guys but I have no choice – if you want bruteforcing... That's going to involve some scripting: let's set a range from 1 to 1000 first, some regexp forfiltering out unsuccessful tries, count an MD5, put it into cookie and ...<br>... first shot.<br>... 1 hour scripting, result after first request<br>... I feel like a kind of idiot<br>but that means last zone is mine !<br>Zone 5:<br>f478c549e37fa33467241d847f862e6f |  |