Metaday 2012-03-09 Lightning talk

Capture the Flag!

By Michael “MiKa” Kafka
@Metalab
@SecurityByCandlelight
@DeepSec

What's a CtF?

- Capture the Flag
  - In our world: Official way to hack, test your skillz (l33t or n00b)
    aka Wargame
    aka Hacking Challenge
  - AFK: Outdoor game with two parties... etc... too much action and exposure to sunlight. Implies physical exhaustion and running around in the dirt.

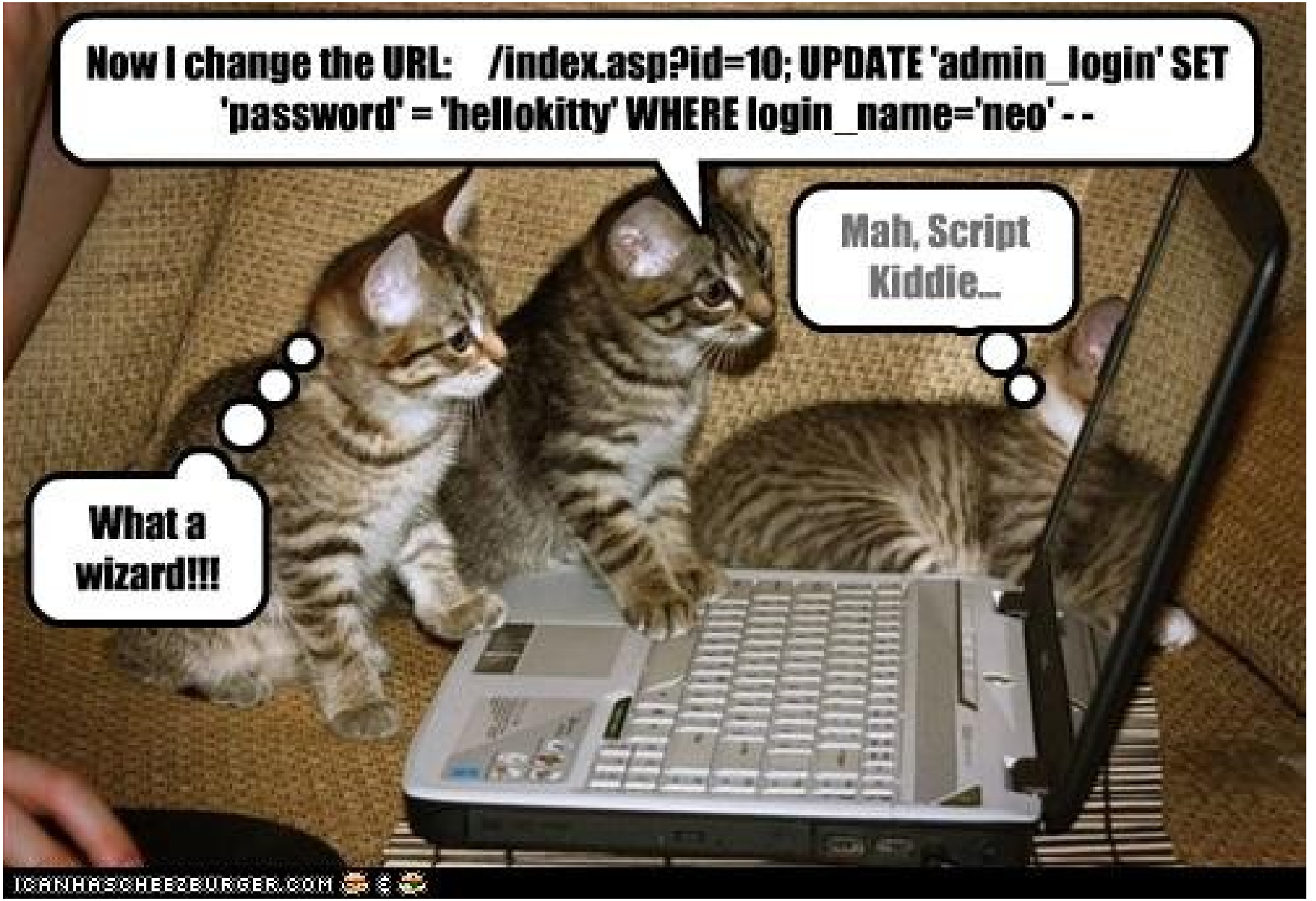
Our First CtF: How it Began

- Surf teh Interwebs...
  - -> Someone spotted a new CtF
  - stripe.com invites to hack stri.pe
- Give it a try!
  - Ooops, suid? Source code is simple... What the heck? How to exploit?
    (My Unix-skillz have deficits...)
- Go to the Metalabs!
  - Hope the find it as funny
    And they did!

The Hack Begins

- Quickly found 5 others
  - Different skills, background, interests=
    - Covering many areas
    - Synergy!
  - Immediate team building
    - Lots of discussions and many ideas
    - Great cooperation
  - Nice about it:
    - No “leadership”
    - Only expertise in specific fields counts

How to start?

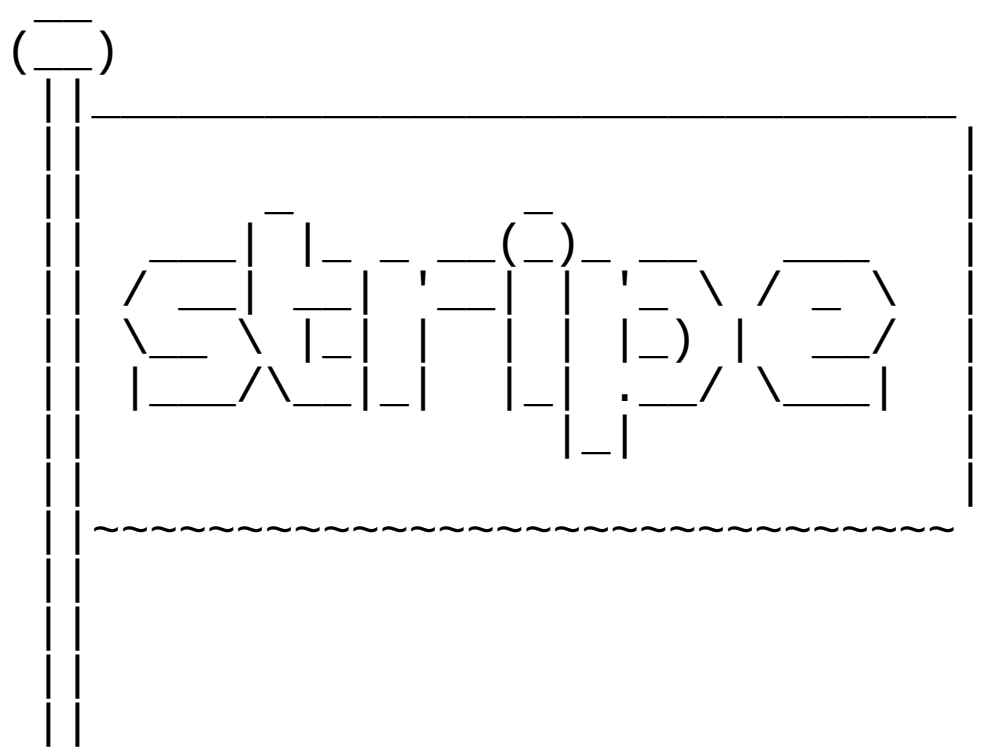

Now I change the URL: /index.asp?id=10; UPDATE 'admin_login' SET 'password' = 'hellokitty' WHERE login_name='neo' - -
Mah, Script Kiddie...
What a wizard!!!
ICANHASCHEEZBURGER.COM

This is How to Do it

What to Achieve?

Our Goal is Simple:

```
----------------------------------------
```



```
Please enter your preferred handle: MetalabLoungeTeam
Welcome, MetalabLoungeTeam!
the-flag@ctf4:/tmp/tmp.3vDFDpVdmH$
```

First Challenge:

- This was quite easy, although I have to admit that the others showed me how to do it. A suid executable was provided and the source code was available.
- Teaser: what will happen, if you enter “date” at the system prompt? Are you sure?

Second Challenge

- Again, simple: A web based attack with the source code available.
- Teaser: Just look carefully, what information is sent to the server. Is it secured?

Third Challenge

- This one was tricky, it’s time to refresh your C-skills. Source code available.
- Teaser: If you can’t jump forward then go back, just make sure you land on the right spot!

Fourth Challenge

- Looks simple but it’s not easy to exploit, a small C-program which allocates a buffer. Again your C-skills are helpful and your knowledge of the memory layout (oh darn when you notice). And seek help from your friends on the internet -they have something what you need.
- Teaser: The longer the slide, the bigger the fun -and again and again and again.

Fifth Challenge

- Oh boy, oh boy: a python client/server web-application. Source provided, looks good and robust. We didn’t find any insecure handling of user provided data. Oh wait…
- Teaser: Can I have a side of pickles with that?

Sixth Challenge (Boss Level)

- That took longer than expected, C-source provided. Char by char password compare, a pretty short buffer to exploit, actually it's not exploitable. Input length validated etc… robust code. This took us longer than expected. We developed two approaches and we made a little race.
- Teaser 1: If the channel you are watching is boring switch to another.
- Teaser 2: If everything is happening too fast, can you make it halt?

Feedback:

- Everyone was excited and enthusiastic
- We had lots of fun
- When do we attack the next?

Citation:

“It took six years of running a hackerspace until we finally got a decent hacking session”

Resumee:

- A clean and safe way to test your hacking skillz
- Nice experience in terms of team building
- Recommended for everyone involved in security, secure coding, penetration testing