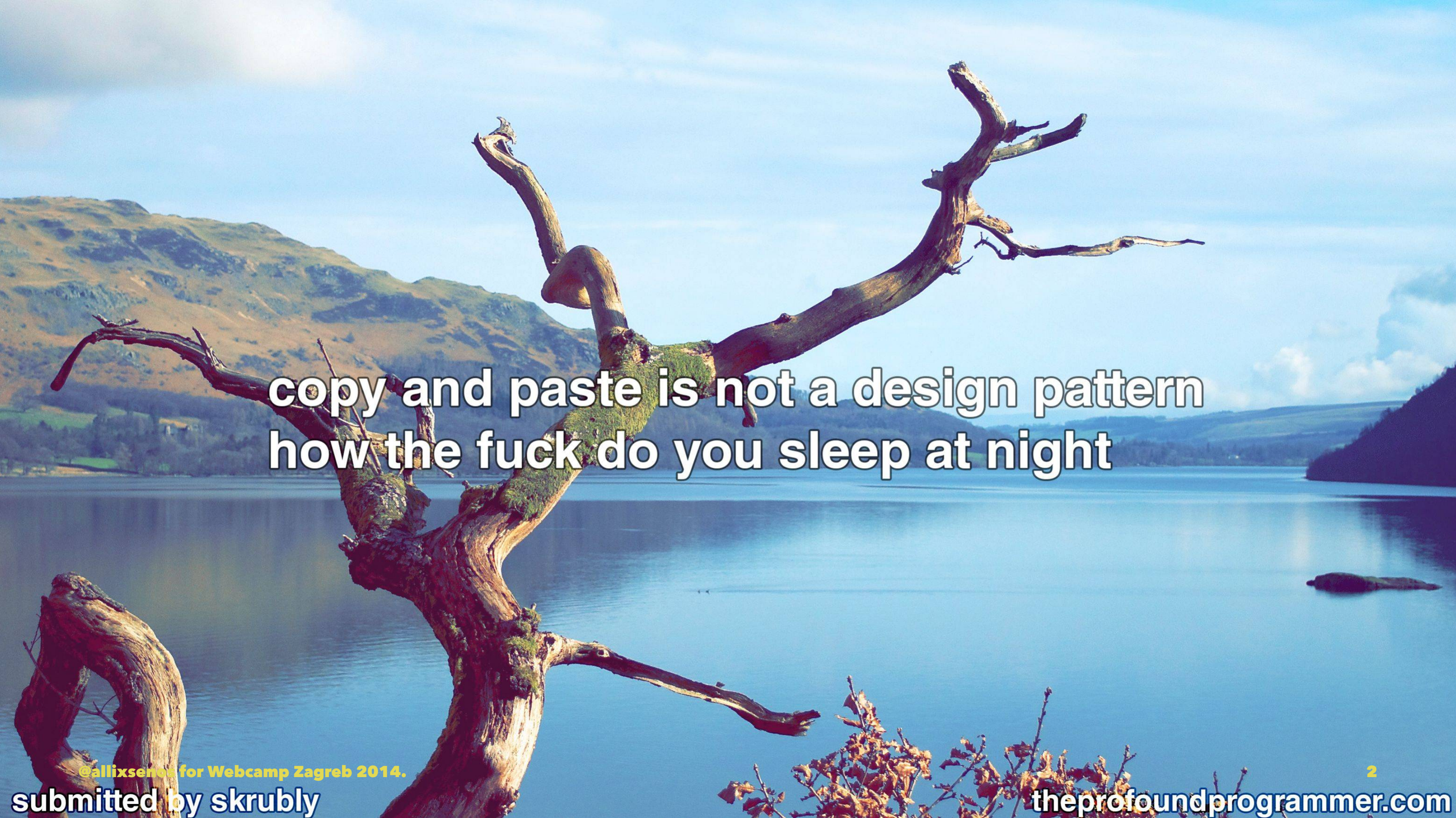
BAD IDEAS
& worst practices

Luka Kladarić
luka@hitlistapp.com
@kll



submitted by skrubly

theprofoundprogrammer.com

Bad ideas

PHP

Worst practices

PHP Frameworks

Any questions?

Kidding.[1]

[1] for the most part.

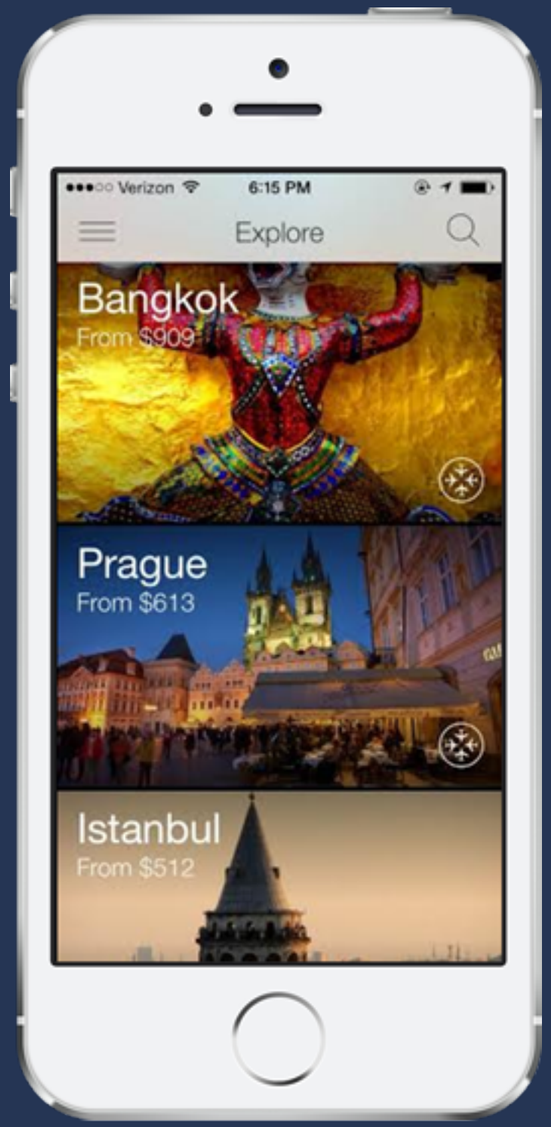
Who?

Luka Kladarić

recovering PHPholic

10+ years of professional webdev (asp, php, js, python)

3 years at deviantART, a megascale web property



CTO at Hitlist, a New York-based travel tech startup

www.hitlistapp.com

a lot of experience breaking things

Bad ideas & worst practices?

Antipatterns.

Lack of skill, experience and insight to recognize a bad solution.

Lack of will to find a better one.

Cowboy coder byproduct.[2]

[2] c2wiki: Cowboy Coder

1) Trusting user input

SQL injection

(and other flavours of injection)

```
SELECT * FROM accounts WHERE custID="{$_GET['id']}"
```

```
http://mysite.com/show_customer.php?id=" OR 1=1; --
```

```
SELECT * FROM accounts WHERE custID="" OR 1=1;
```

used to bypass login and permissions, leak sensitive information, extract entire databases... possibilities endless

shellshock

```
$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
$
```

and various other uninentional and malicious exploits from unchecked user input

2) Trusting the middleware

(browsers/apps, protocols, proxies, ...)

Cookies & sessions

```
Set-Cookie: userid=32742427;
```

- hmmmm, I wonder what happens if I change the `id`?
- store as little as possible
- encrypt/sign to protect against tampering
- because people WILL tamper with them

Cookies & sessions

```
Cookie: userid=SOMEONE_ELSE;
```

1. log into the game as someone else
2. sell their rare valuables on the marketplace
3. log in as me from a different browser & buy them
4. MUAHAHA.

The apps don't work for you

```
<input type="text" name="SPARE_POINTS" value="0" readonly>

<input type="text" name="STRENGTH" value="10" readonly> <button>+</button>
<input type="text" name="DEXTERITY" value="10" readonly> <button>+</button>
<input type="text" name="CONSTITUTION" value="10" readonly> <button>+</button>
<input type="text" name="INTELLIGENCE" value="10" readonly> <button>+</button>
    (circa 2004)
```

the text fields are "read only", the buttons distribute SPARE_POINTS, what could possibly go wrong?

```
<input type="text" name="SPARE_POINTS" value="0" readonly>

<input type="text" name="STRENGTH" value="1000" blabla> <button>+</button>
<input type="text" name="DEXTERITY" value="1000" blabla> <button>+</button>
<input type="text" name="CONSTITUTION" value="1000" blabla> <button>+</button>
<input type="text" name="INTELLIGENCE" value="1000" blabla> <button>+</button>
```

that didn't actually work

they EXPECTED IT

but...

```
<input type="text" name="SPARE_POINTS" value="0" readonly>

<input type="text" name="STRENGTH" value="440"> <button>+</button>
<input type="text" name="DEXTERITY" value="300"> <button>+</button>
<input type="text" name="CONSTITUTION" value="300"> <button>+</button>
<input type="text" name="INTELLIGENCE" value="-1000"> <button>+</button>
```

now that worked.

I have successfully used in-transit or in-browser tampering to:

1. obtain an expenses-covered invitation to a sporting event on a different continent[3]

[3] didn't actually **use** it (or give my real info)

2. get to the top of the leaderboard in 5 minutes, in a game I've been playing for months and was #140 on the list

3. buy stuff from / have it shipped to Croatia when it wasn't on the supported countries list

4. pay less for goods or services

5. get better air travel prices

never, ever, trust anything that may have originated outside your system

3) passwords

id	username	password
1	admin	admin
2	joe	admin
3	moe	moe
4	freddie	123456
5	wilma	moe

id	username	MD5(password)
1	admin	21232f297a57a5a743894a0e4a801fc3
2	joe	21232f297a57a5a743894a0e4a801fc3
3	moe	7f33334d4c2f6dd6ffc701944cec2f1c
4	freddie	e10adc3949ba59abbe56e057f20f883e
5	wilma	7f33334d4c2f6dd6ffc701944cec2f1c

id	username	MD5("salted"+password)
1	admin	886023aadcd890a53976ea52a2c6866f
2	joe	886023aadcd890a53976ea52a2c6866f
3	moe	664c3b4abe62bcfa3573b8e5dd8b2608
4	freddie	7787501ba5fb91c673983437be99e177
5	wilma	664c3b4abe62bcfa3573b8e5dd8b2608

id	username	MD5("salted"+username+password)
1	admin	328dd00fe4630672b17c5076d8f26f9b
2	joe	2b9ec8e996d1325a8d82c0687eb5ec49
3	moe	9b20e3736d939cc51893a24175a4635d
4	freddie	1a17c349bb81758b8f576800a7dfa89e
5	wilma	af72a08de64db30fae66fed8ae024836

Hash	Type	Result
21232f297a57a5a743894a0e4a801fc3	md5	admin
7f33334d4c2f6dd6ffc701944cec2f1c	md5	moe
e10adc3949ba59abbe56e057f20f883e	md5	123456
886023aadcd890a53976ea52a2c6866f	Unknown	Not Found
664c3b4abe62bcfa3573b8e5dd8b2608	Unknown	Not Found
7787501ba5fb91c673983437be99e177	Unknown	Not Found
328dd00fe4630672b17c5076d8f26f9b	Unknown	Not Found
2b9ec8e996d1325a8d82c0687eb5ec49	Unknown	Not Found
9b20e3736d939cc51893a24175a4635d	Unknown	Not Found
1a17c349bb81758b8f576800a7dfa89e	Unknown	Not Found

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

4) inventing your own wheel

a sure-fire recipe for ending up on this list is to reinvent something that already exists

like rolling your own ID generation system for the database

and then doing a

TALK

about it

- Common task:

  Insert a new record with ID field

- Typical solutions:
  - Use auto-increment field and
    fetch last ID value after the insert
    → race conditions and context problems

  - Use auto-increment field and
    read back record after insert based on u
    → performance overhead

- Common task:

  Insert a new record with ID field

- Better solution:

  - Use big integer field as ID and
    insert a random ID number

  - In case of duplicates (hardly ever happens),
    simply retry the insert with a new random number


REALLY?

databases have been generating IDs since before you heard of databases. leave Britney alone.

so...

how to NOT end up on this list?

surround yourself with people smarter than you

show them what you're working on

listen when they tear it apart


do it again.

Questions?

(for real)

Thank you!

@allixsenos

luka@hitlistapp.com