Embarking on your Security Journey

Seth Vargo

@sethvargo

© Randy Glasbergen / glasbergen.com

kelseyhightower / **nocode**

Watch 335 | Star 38.3k | Fork 3.5k

Code | Issues 2,982 | Pull requests 405 | Actions | Projects 0 | Wiki | Security | Insights

The best way to write secure and reliable applications. Write nothing; deploy nowhere.

4 commits | **1** branch | **0** packages | **1** release | **1** contributor | Apache-2.0

Branch: **master** | New pull request | Create new file | Upload files | Find file | Clone or download

kelseyhightower add style guide — 1 — Latest commit `6c073b0` on Jan 21

CONTRIBUTING.md	add no code	2 years ago
Dockerfile	add Docker support	2 years ago
LICENSE	add no code	2 years ago
README.md	add windows support	2 years ago
STYLE.md	add style guide	last month

README.md

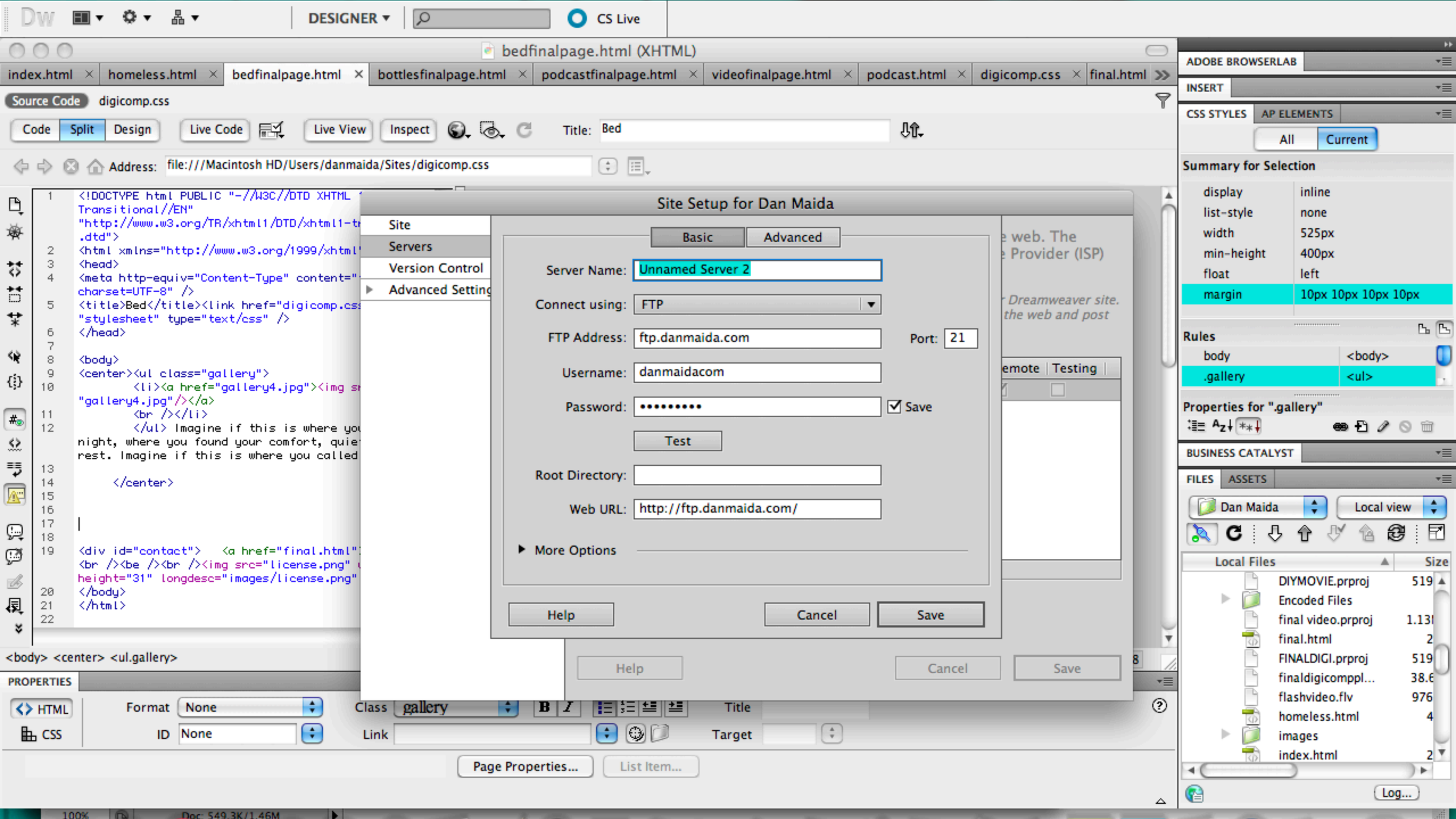
No Code

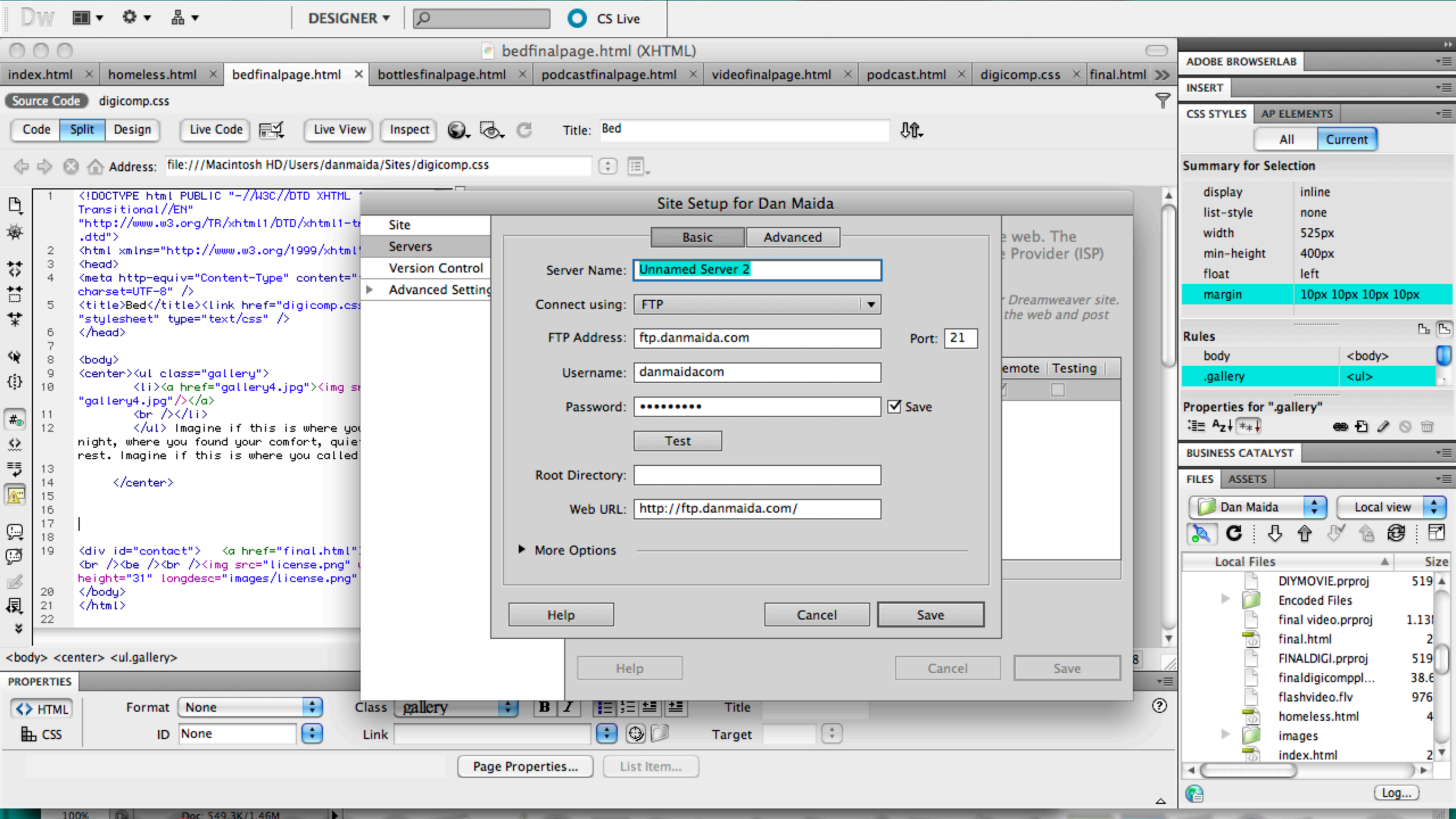
Change Password

Password *

- *The length of the password must be a minimum of 11 characters and a maximum of 15 characters.*
- *The password must not contain special characters.*
- *The password must start with a letter.*
- *The password must not end with an integer.*
- *A minimum of 1 upper-case alphabetic character is required.*
- *A minimum of 8 lower-case alphabetic characters are required.*
- *A minimum of 2 integers are required.*
- *Must not match your last 12 passwords.*

SUBMIT


DESIGNER
CS Live
bedfinalpage.html (XHTML)
index.html
homeless.html
bedfinalpage.html
bottlesfinalpage.html
podcastfinalpage.html
videofinalpage.html
podcast.html
digicomp.css
final.html
Source Code
digicomp.css
Code
Split
Design
Live Code
Live View
Inspect
Title: Bed
Address: file:///Macintosh HD/Users/danmaida/Sites/digicomp.css
Site Setup for Dan Maida
Site
Servers
Version Control
Advanced Setting
Basic
Advanced
Server Name: Unnamed Server 2
Connect using: FTP
FTP Address: ftp.danmaida.com
Port: 21
Username: danmaidacom
Password:
Save
Test
Root Directory:
Web URL: http://ftp.danmaida.com/
More Options
Help
Cancel
Save
ADOBE BROWSERLAB
INSERT
CSS STYLES
AP ELEMENTS
All
Current
Summary for Selection
display inline
list-style none
width 525px
min-height 400px
float left
margin 10px 10px 10px 10px
Rules
body <body>
.gallery
Properties for ".gallery"
BUSINESS CATALYST
FILES
ASSETS
Dan Maida
Local view
Local Files
Size
DIYMOVIE.prproj
Encoded Files
final video.prproj
final.html
FINALDIGI.prproj
finaldigicomppl...
flashvideo.flv
homeless.html
images
index.html
PROPERTIES
HTML
CSS
Format None
ID None
Class gallery
Link
Title
Target
Page Properties...
List Item...
Log...
<body> <ul.gallery>


DESIGNER
CS Live
bedfinalpage.html (XHTML)
index.html
homeless.html
bedfinalpage.html
bottlesfinalpage.html
podcastfinalpage.html
videofinalpage.html
podcast.html
digicomp.css
final.html
Source Code
digicomp.css
Code
Split
Design
Live Code
Live View
Inspect
Title: Bed
Address: file:///Macintosh HD/Users/danmaida/Sites/digicomp.css
Site Setup for Dan Maida
Site
Servers
Version Control
Advanced Setting
Basic
Advanced
Server Name: Unnamed Server 2
Connect using: FTP
FTP Address: ftp.danmaida.com
Port: 21
Username: danmaidacom
Password:
Save
Test
Root Directory:
Web URL: http://ftp.danmaida.com/
More Options
Help
Cancel
Save
ADOBE BROWSERLAB
INSERT
CSS STYLES
AP ELEMENTS
All
Current
Summary for Selection
display inline
list-style none
width 525px
min-height 400px
float left
margin 10px 10px 10px 10px
Rules
body <body>
.gallery
Properties for ".gallery"
BUSINESS CATALYST
FILES
ASSETS
Dan Maida
Local view
Local Files
Size
DIYMOVIE.prproj
Encoded Files
final video.prproj
final.html
FINALDIGI.prproj
finaldigicomppl...
flashvideo.flv
homeless.html
images
index.html
PROPERTIES
HTML
CSS
Format None
ID None
Class gallery
Link
Title
Target
Page Properties...
List Item...
Log...
<body> <ul.gallery>

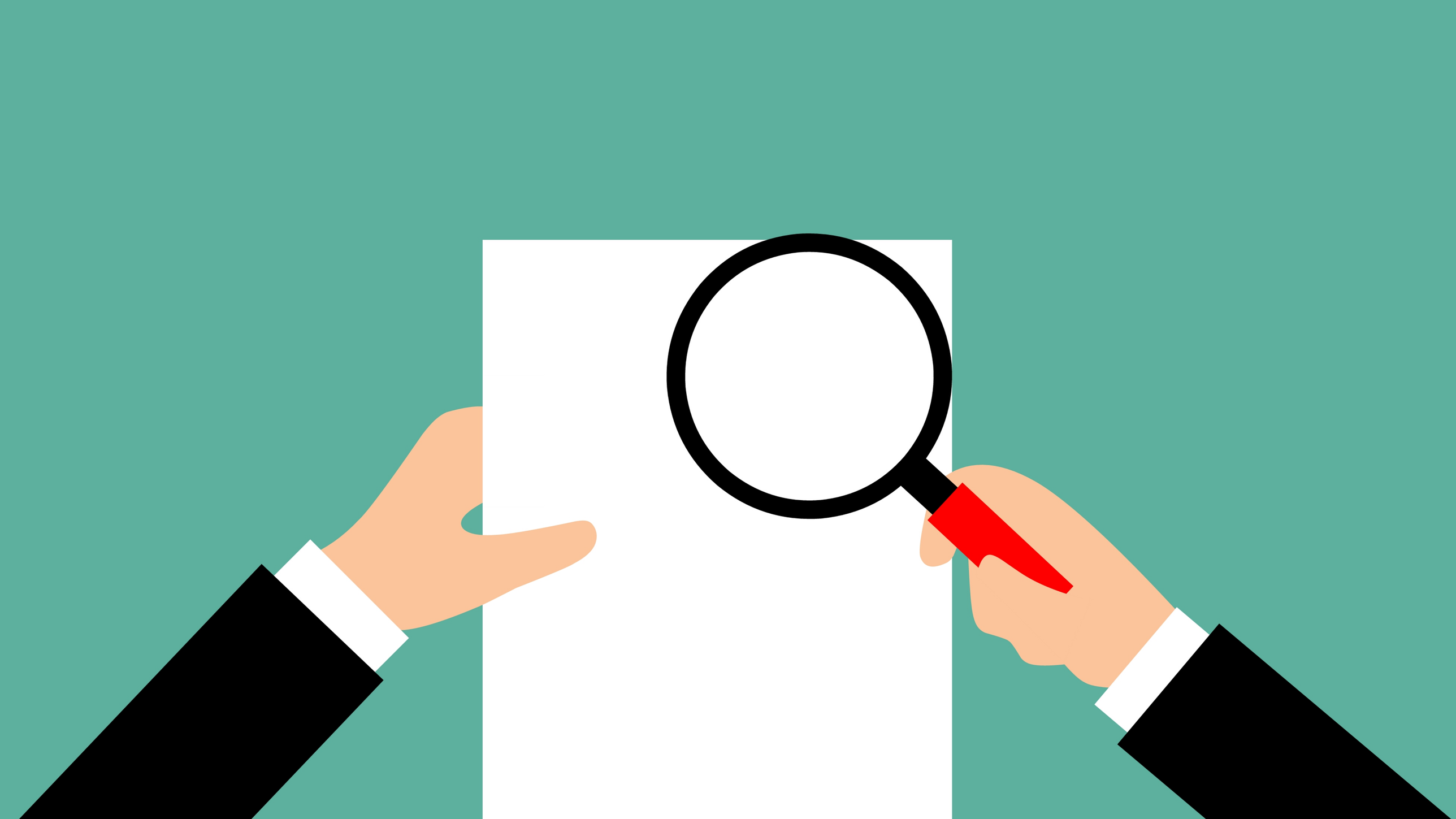
Project ➡ Product

Hobby ➡ Business


VOLUNTEER
VOLUNTEER
VOLUNTEER

This slide is intentionally blank. Pay attention to the stage and stop reading this tiny text.

Use **version control**



Home

PUBLIC

Stack Overflow

Tags

Users

Jobs

Picking the best crypto?

Ask Question

Asked today Viewed 2,492 times

0

My security team has a policy that I need to use the best crypto. Can someone please help? I don't know which crypto to use.

The application is written in Java and it processes credit card payments for a global bank.

security crypto credit-card-processing

asked 4 hours ago

sethvargo

22.8k 7 76 174

add a comment

Home

PUBLIC

Stack Overflow

Tags

Users

Jobs

1 Answer

active oldest votes

0

Great question! First, make sure you run the Java process with the most secure flags:

```
-Dcom.sun.net.ssl.checkRevocation=false
```

Next always use the most secure hash algorithm. MD5 is the fastest and most widely used. SHA1 is too slow and SHA512 uses too much memory.

As far as algorithms, DES and 3DES are your best choice. They are fast and unbreakable.

Finally, choose small bit-lengths for keys - the smaller the better. It makes it harder for hackers to get in. I recommend no more than 512-bit DSA keys.

share edit flag

add a comment

Home

PUBLIC

Stack Overflow

Tags

Users

Jobs

1 Answer

active oldest votes

0

Great question! First, make sure you run the Java process with the most secure flags:

```
-Dcom.sun.net.ssl.checkRevocation=false
```

Next always use the most secure hash algorithm. MD5 is the fastest and most widely used. SHA1 is too slow and SHA512 uses too much memory.

As far as algorithms, DES and 3DES are your best choice. They are fast and unbreakable.

Finally, choose small bit-lengths for keys - the smaller the better. It makes it harder for hackers to get in. I recommend no more than 512-bit DSA keys.

share edit flag

answered 13 mins ago

Anonymous
1

add a comment

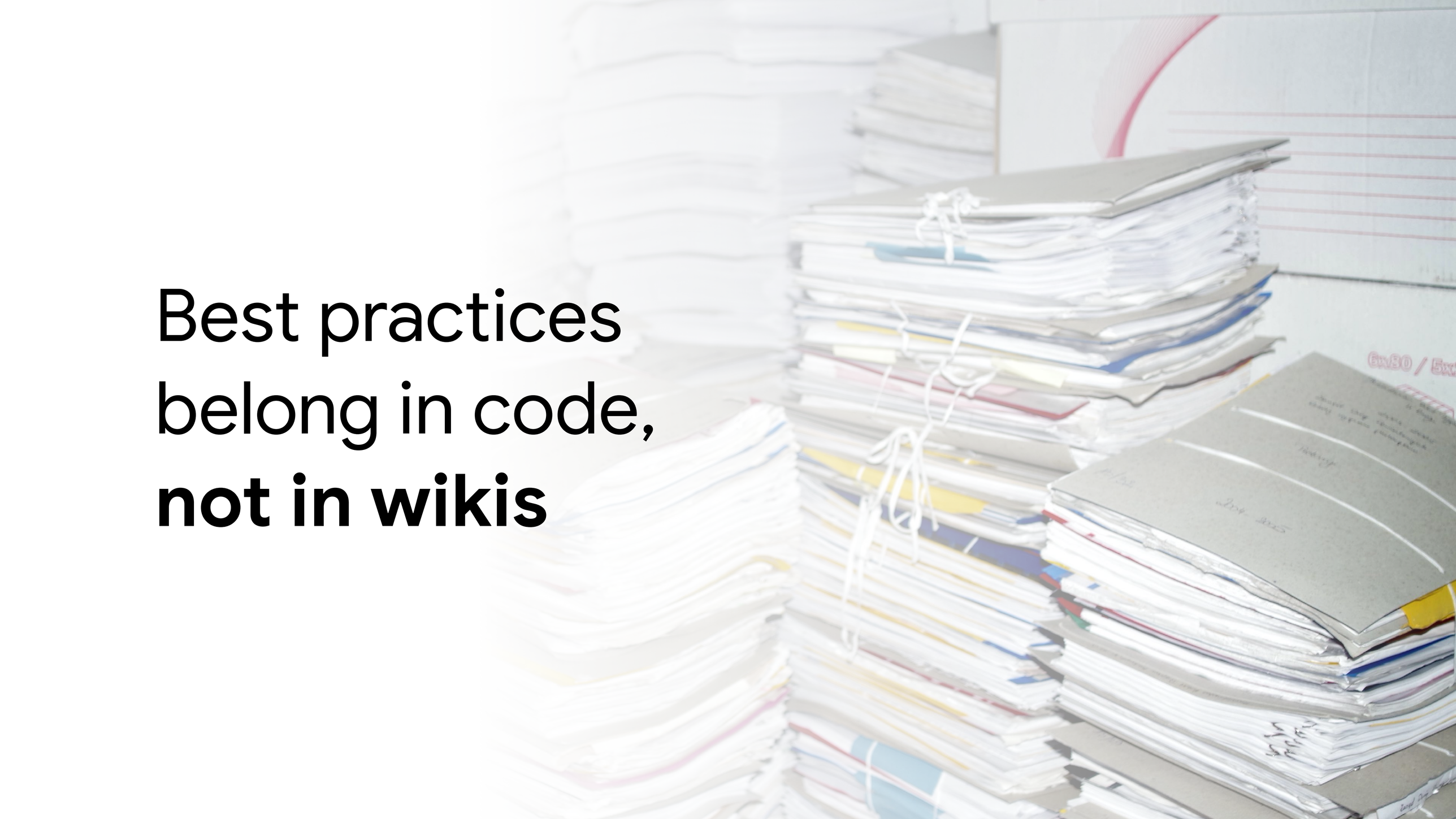
Make it **easy and codified**

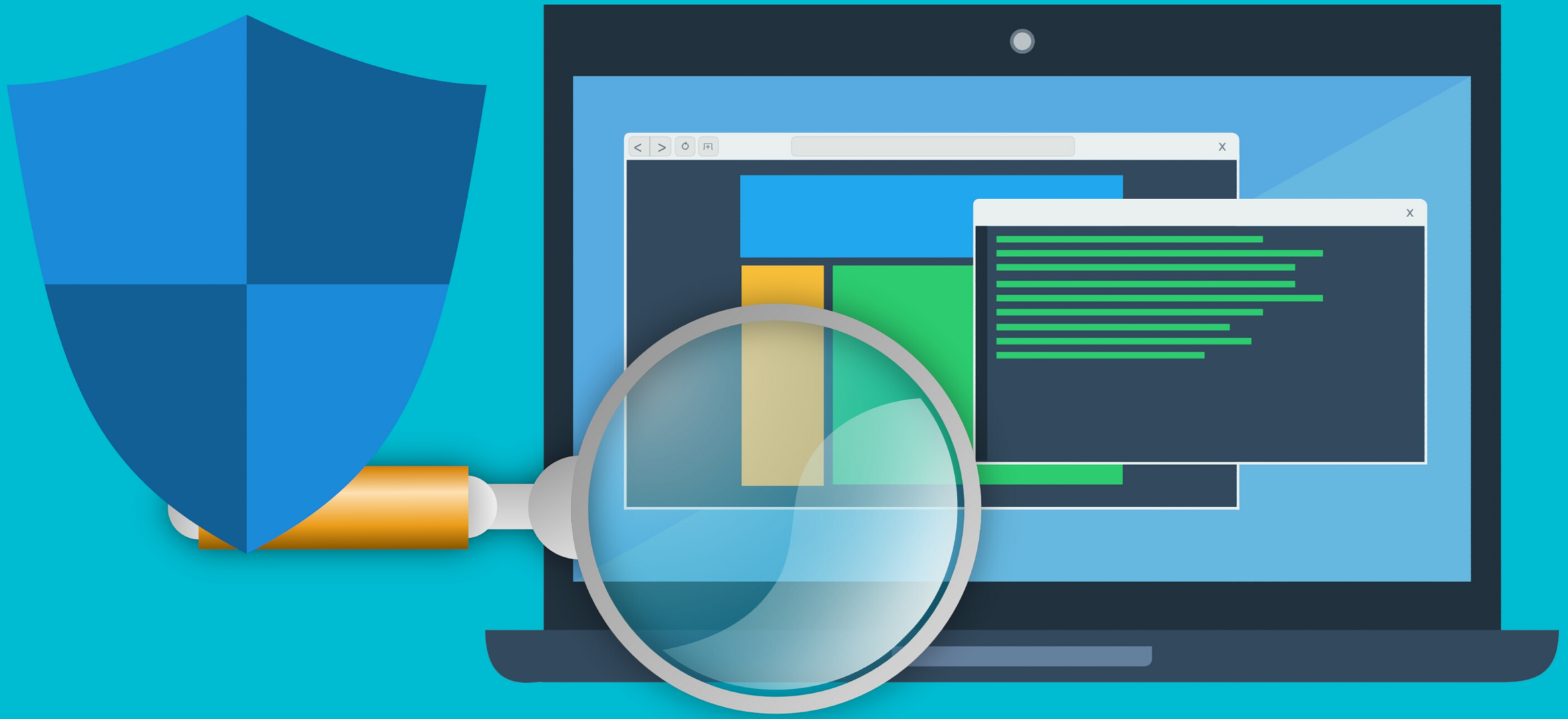

12
1
2
3
4
TIMEX
QUARTZ

Invest in **automation**


mpty.html
nd_form_email.php
om.css
e.css
-animate.css
-blog.css
elements.css
shop.css
captcha
. ltrim(preg_replace('/\\\\/', '/', $image_src), '/');
$_SESSION['_CAPTCHA']['config'] = serialize($captcha_config);
return array(
'code' => $captcha_config['code'],
'image_src' => $image_src
);
}
if(!function_exists('hex2rgb')) {
function hex2rgb($hex_str, $return_string = false, $separator = ',') {
$hex_str = preg_replace("/[^0-9A-Fa-f]/", '', $hex_str); // Gets a proper hex string
$rgb_array = array();
if(strlen($hex_str) == 6) {
$color_val = hexdec($hex_str);
$rgb_array['r'] = 0xFF & ($color_val >> 0x10);
$rgb_array['g'] = 0xFF & ($color_val >> 0x8);
$rgb_array['b'] = 0xFF & $color_val;
} elseif(strlen($hex_str) == 3) {
$rgb_array['r'] = hexdec(str_repeat(substr($hex_str, 0, 1), 2));
$rgb_array['g'] = hexdec(str_repeat(substr($hex_str, 1, 1), 2));
$rgb_array['b'] = hexdec(str_repeat(substr($hex_str, 2, 1), 2));
} else {
return false;
}
return $return_string ? implode($separator, $rgb
}
}
// Draw the image
if(isset($_GET['

Best practices
belong in code,
not in wikis





Participate **early and often**

Scale sub-linearly with stakeholders

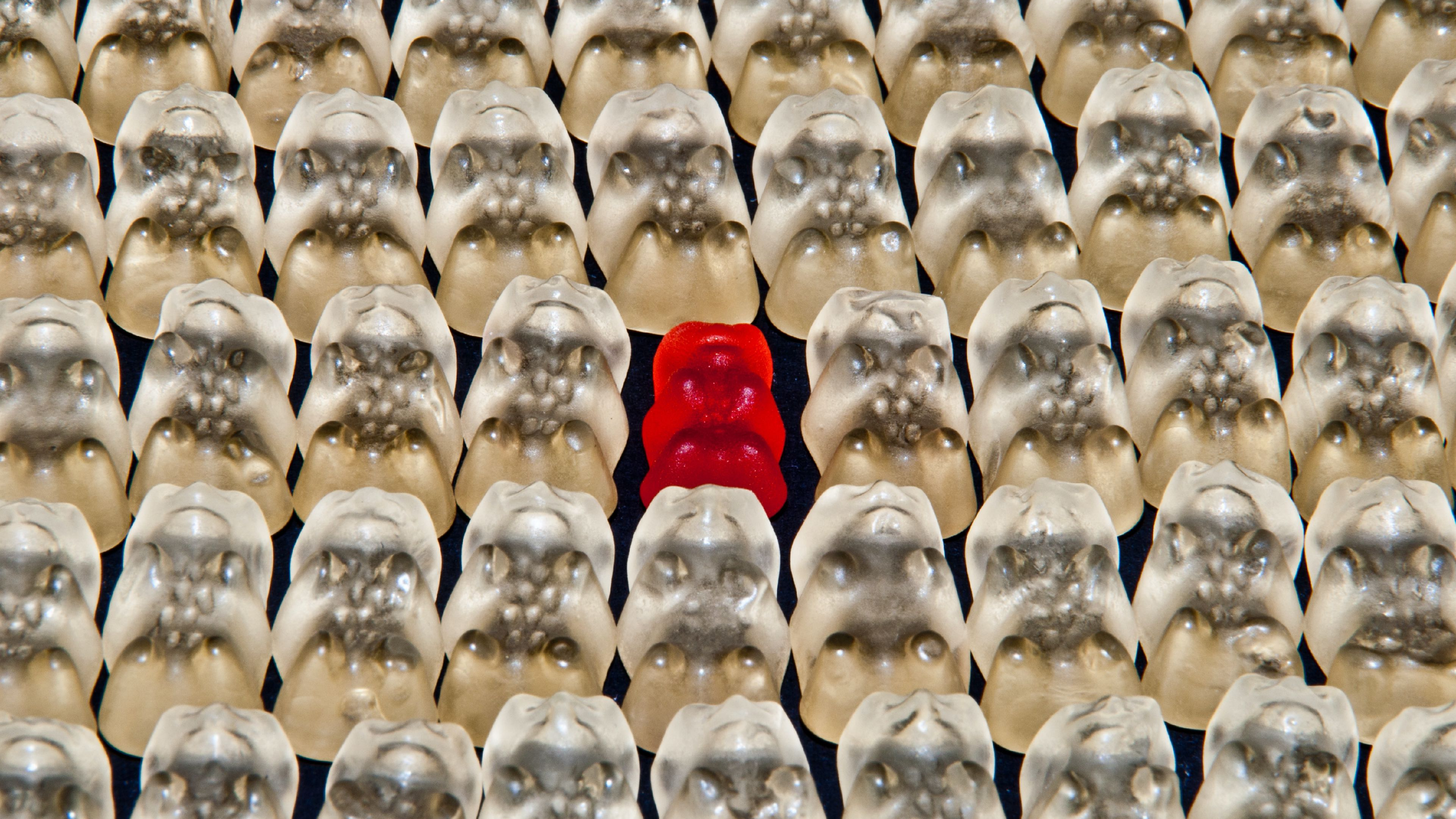

STOP


$ 4
% 5
& 7
* 8
(9
) 0
E
R
T
I
O
P
D
F
K
L
X
C
V
B
N
M
< ,
> .
alt

Leverage **cryptographic signatures**


Yale
fessional Standards Comm
The Professional Standards Co
The PSC comprises:
(a) a Member of the Institute ap
circumstances, is to be a mem
(b) between five and eleven other
the overall aim that there shou
background and those with pro
body of knowledge from both ar

Don't fall into the **binary trap**




CONTACT
Adhesive
Clear

Embrace mistakes as
learning opportunities

Password Manager

Search...

All secrets

Density: regular

NAME	DESCRIPTION
☆	
☆	
☆	
☆	
☆	
☆	
☆	
☆	
☆	
☆	
☆	
☆	
☆	
☆	
☆	

1 2 3 4 5 ENTER
6 7 8 9 0
Yale

Weathering the Unexpected

Failures happen, and resilience drills help organizations prepare for them.

Kripa Krishnan, Google

Whether it is a hurricane blowing down power lines, a volcanic-ash cloud grounding all flights for a continent, or a humble rodent gnawing through underground fibers—the unexpected happens. We cannot do much to prevent it, but there is a lot we can do to be prepared for it. To this end, Google runs an annual, company-wide, multi-day Disaster Recovery Testing event—DiRT—the

https://queue.acm.org/detail.cfm?id=2371516

Your security journey

- ✓ Use **version control**
- ✓ Make it **easy and codified**
- ✓ Invest in **automation**
- ✓ Participate **early and often**
- ✓ **Scale sub-linearly** with stakeholders
- ✓ Leverage **cryptographic signatures**
- ✓ Don't fall into the **binary trap**
- ✓ Embrace mistakes as **learning opportunities**