

# WEB PENETRATION TESTING

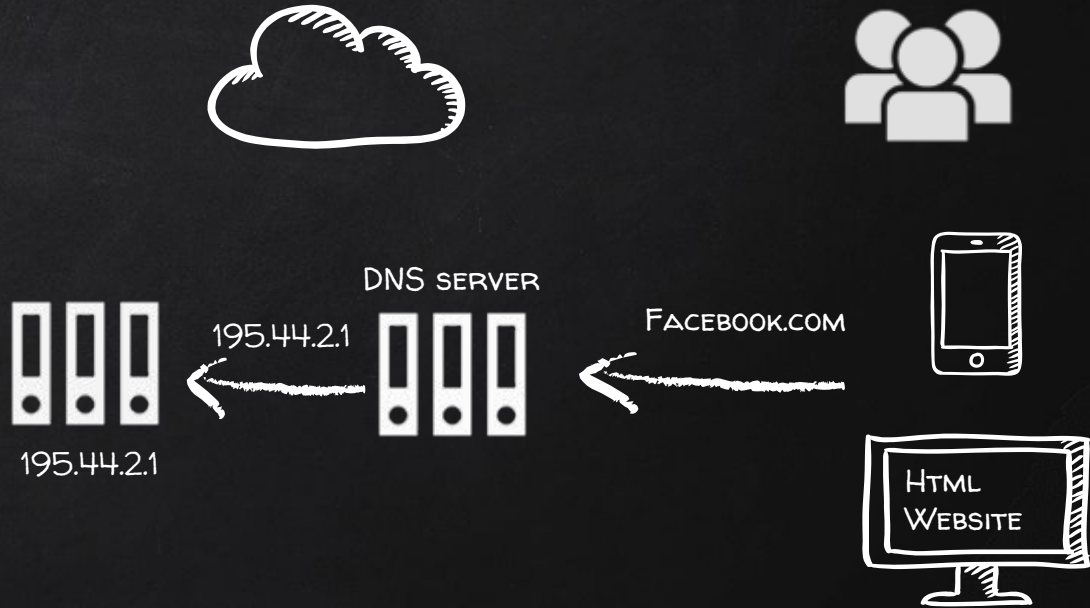
---



# WHAT IS A WEBSITE

## HOW TO HACK A WEBSITE?

- Computer with OS and some servers.
- Apache, MySQL ...etc
- Contains web application.
- PHP, Python ...etc
- Web application is executed here and not on the client's machine



# WHAT IS A WEBSITE

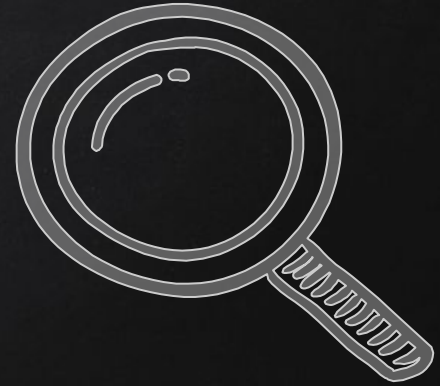
## HOW TO HACK A WEBSITE?

- An application installed on a computer . → web application pentesting
- Computer uses an OS + other applications → server side attacks.
- Managed by humans → client side attacks.



# INFORMATION GATHERING

- IP address.
- Domain name info.
- Technologies used.
- Other websites on the same server.
- DNS records.
- Unlisted files, sub-domains, directories.



# INFORMATION GATHERING

1. Whois Lookup – Find info about the owner of the target.  
→ <http://whois.domaintools.com/>
2. Netcraft Site Report – Shows technologies used on the target.  
→ [http://toolbar.netcraft.com/site\\_report?url=](http://toolbar.netcraft.com/site_report?url=)
3. Robtex DNS lookup – Shows comprehensive info about the target website.  
→ <https://www.robtex.com/>

# INFORMATION GATHERING

## WEBSITES ON THE SAME SERVER

- One server can serve a number of websites.
- Gaining access to one can help gaining access to others.

To find websites on the same server:

1. Use Robtex DNS lookup under “names pointing to same IP”.
2. Using bing.com, search for ip: [target ip]

# INFORMATION GATHERING

## SUBDOMAINS

- Subdomain.target.com
- Ex: beta.facebook.com

Knock can be used to find subdomains of target

1. Download it `> git clone https://github.com/guelfoweb/knock.git`
2. Navigate to knock.py. `> cd knock/knock.py`
3. Run it `> python knock.py [target]`

# INFORMATION GATHERING

## FILES + DIRECTORIES

- Find files & directories in target website
- A tool called dirb.

```
> dirb [target] [wordlist] [options]
```

For more info run

```
> man dirb
```



# EXPLOITATION

## FILE UPLOAD VULNS



- Simple type of vulnerabilities.
- Allow users to upload executable files such as php.

Upload a php shell or backdoor, ex: weevly

1. Generate backdoor `> weevly generate [passord] [file name]`
2. Upload generated file.
3. Connect to it `> weevly [url to file] [password]`
4. Find out how to use weevly `> help`

# EXPLOITATION

## CODE EXECUTION VULNS



- Allows an attacker to execute OS commands.
- Windows or linux commands.
- Can be used to get a reverse shell.
- Or upload any file using wget command.
- Code execution commands attached in the resources.

# EXPLOITATION

## LOCAL FILE INCLUSION



- Allows an attacker read ANY file on the same server.
- Access files outside www directory.

# EXPLOITATION

## REMOTE FILE INCLUSION



- Similar to local file inclusion.
- But allows an attacker read ANY file from ANY server.
- Execute php files from other servers on the current server.
- Store php files on other servers as .txt



# MITIGATION



1. File Upload Vulns – Only allow safe files to be uploaded.
2. Code Execution Vulns:
  - Don't use dangerous functions.
  - Filter user input before execution.
3. File inclusion:
  - Disable `allow_url_fopen` & `allow_url_include`.
  - Use static file inclusion.

# EXPLOITATION – SQL INJECTION

## WHAT SQL ?

- Most websites use a database to store data.
- Most data stored in it (usernames, passwords ..etc)
- Web application reads, updates and inserts data in the database.
- Interaction with DB done using **SQL**.



# EXPLOITATION – SQL INJECTION

## WHY ARE THEY SO DANGEROUS

1. They are everywhere.
2. Give access to the database → sensitive data.
3. Can be used to read local files outside www root.
4. Can be used to log in as admin and further exploit the system.
5. Can be used to upload files.



# EXPLOITATION – SQL INJECTION

## DISCOVERING SQLI

- Try to break the page.
- Using 'and', 'order by' or “”.
- Test text boxes and url parameters on the form  
<http://target.com/page.php?something=something>





# EXPLOITATION – SQL INJECTION

## SQLMAP

- Tool designed to exploit sql injections.
- Works with many db types, mysql, mssql ...etc.
- Can be used to perform everything we learned and more!

```
> sqlmap --help  
> sqlmap -u [target url]
```



# PREVENTING SQLI



- Filters can be bypassed.
- Use black list of commands? Still can be bypassed
- Use whitelist? Same issue

→ Use parameterized statements, separate data from sql code.

# EXPLOITATION – XSS VULNS

## XSS – CROSS SITE SCRIPTING VULNS

- Allow an attacker to inject javascript code into the page.
- Code is executed when the page loads.
- Code is executed on the **client** machine not the server.

Three main types:

1. Persistent/Stored XSS
2. Reflected XSS
3. DOM based XSS

XSS  
Cross Site Scripting

# EXPLOITATION – XSS VULNS

## DISCOVERING XSS

- Try to inject javascript code into the pages.
- Test text boxes and url parameters on the form  
<http://target.com/page.php?something=something>

XSS  
Cross Site Scripting



# EXPLOITATION – XSS VULNS

## REFLECTED XSS

- None persistent, not stored.
- Only work if the target visits a specially crafted URL
- EX

[http://target.com/page.php?something=<script>alert\(“XSS”\)</script>](http://target.com/page.php?something=<script>alert(“XSS”)</script>)

XSS  
Cross Site Scripting

# EXPLOITATION – XSS VULNS

## STORED XSS

- Persistent, stored on the page or DB.
- The injected code is executed everytime the page is loaded.

XSS  
Cross Site Scripting

# EXPLOITATION – XSS VULNS

## EXPLOITING XSS

- Run any javascript code.
- Beef framework can be used to hook targets.
- Inject Beef hook in vulnerable pages.
- Execute code from beef.

XSS  
Cross Site Scripting

# PREVENTING XSS VULNS



- Minimize the usage of user input on html.
- Escape any untrusted input before inserting it into the page.

Char	Result
&	→ &amp;
<	→ &lt;
>	→ &gt;
"	→ &quot;
'	→ &#x27;
/	→ &#x2F;

→ [https://www.owasp.org/index.php/XSS\\_\(Cross\\_Site\\_Scripting\)\\_Prevention\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)



# ZED ATTACK PROXY ZAP

- Automatically find vulnerabilities in web applications.
- Free and easy to use.
- Can also be used for manual testing.





Quotations are commonly  
printed as a means of inspiration  
and to invoke philosophical  
thoughts from the reader.



Bring the attention of your audience over a  
key concept using icons or illustrations



## YOU CAN ALSO SPLIT YOUR CONTENT

### **White**

Is the color of milk and fresh snow, the color produced by the combination of all the colors of the visible spectrum.

### **Black**

Is the color of coal, ebony, and of outer space. It is the darkest color, the result of the absence of or complete absorption of light.



# A PICTURE IS WORTH A THOUSAND WORDS



A complex idea can be conveyed with just a single still image, namely making it possible to absorb large amounts of data quickly.



A vibrant field of red poppies in full bloom, with green stems and leaves visible. The background is a soft-focus expanse of more poppies. A white, hand-drawn rectangular border is centered in the image, containing the text.

WANT BIG  
IMPACT?  
USE BIG  
IMAGE.



## USE CHARTS TO EXPLAIN YOUR IDEAS





## AND TABLES TO COMPARE DATA

	A	B	C
Yellow	10	20	7
Blue	30	15	10
Orange	5	24	16





# MAPS





89,526,124

---

Whoa! That's a big number, aren't you proud?



89,526,124\$

That's a lot of money

185,244 USERS

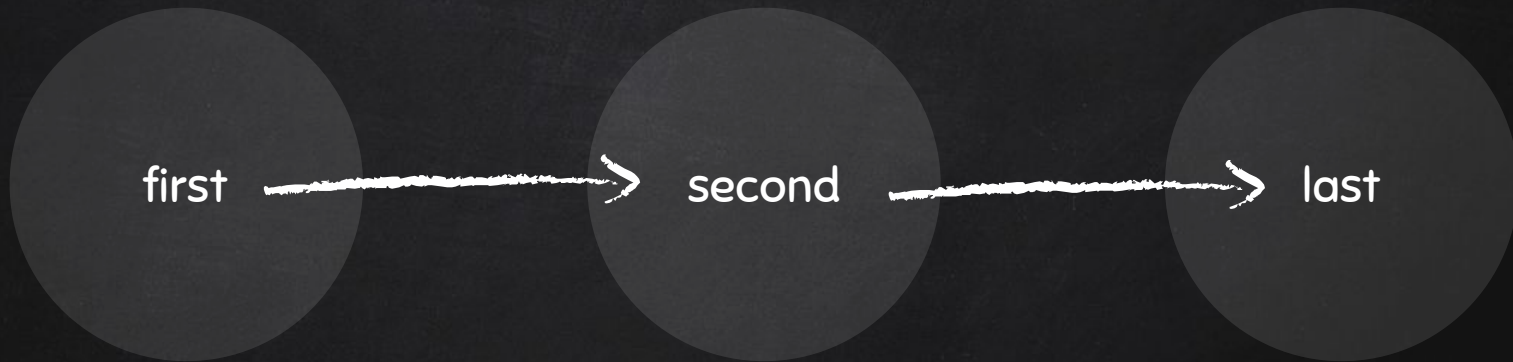
And a lot of users

100%

Total success!



OUR PROCESS IS EASY





## LET'S REVIEW SOME CONCEPTS

### **Yellow**

Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

### **Blue**

Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

### **Red**

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.

### **Yellow**

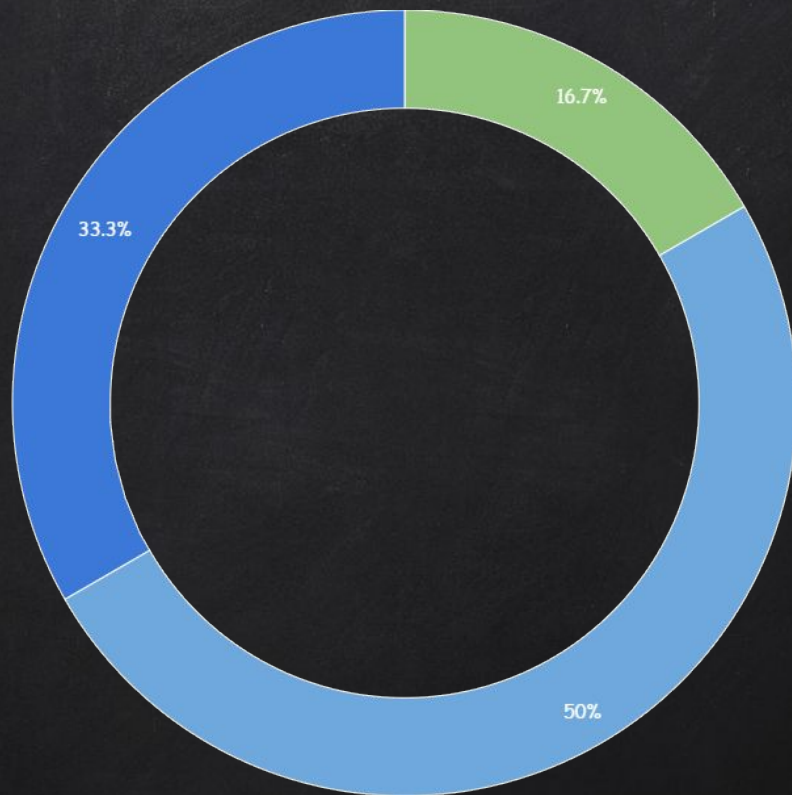
Is the color of gold, butter and ripe lemons. In the spectrum of visible light, yellow is found between green and orange.

### **Blue**

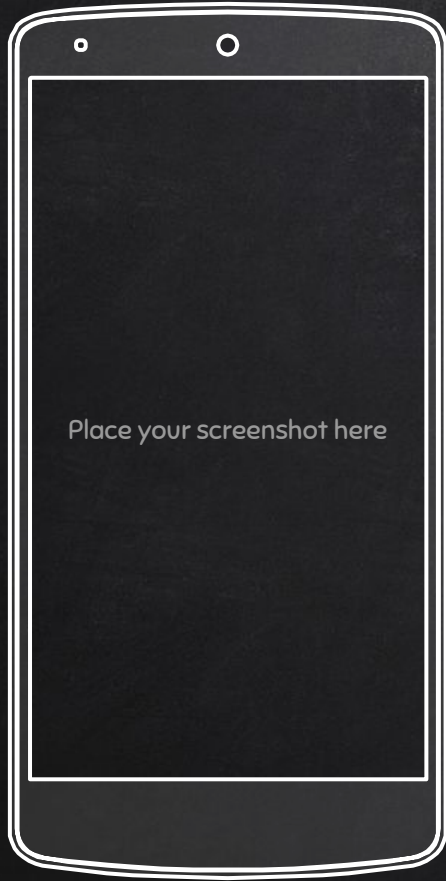
Is the colour of the clear sky and the deep sea. It is located between violet and green on the optical spectrum.

### **Red**

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.



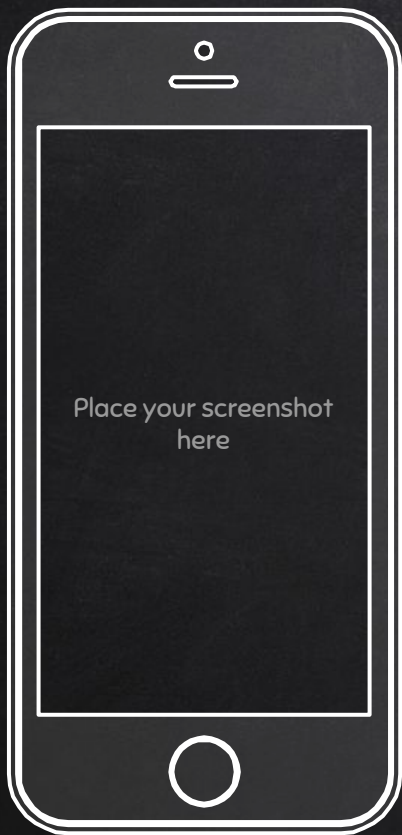
You can copy&paste graphs from Google Sheets



## ANDROID PROJECT

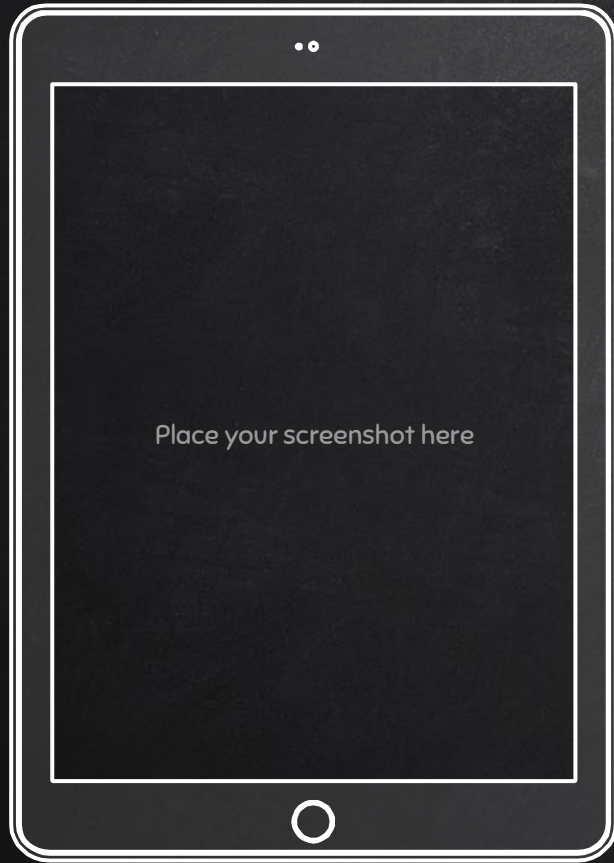
Show and explain your web, app or software projects using these gadget templates.





## IPHONE PROJECT

Show and explain your web, app or software projects using these gadget templates.



## TABLET PROJECT

Show and explain your web, app or software projects using these gadget templates.



## DESKTOP PROJECT

Show and explain your web, app or software projects using these gadget templates.



THANKS!

**Any questions?**

You can find me at  
@username  
user@mailme

## CREDITS

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash



# PRESENTATION DESIGN

This presentation uses the following typographies and colors:

- Titles: Walter Turncoat
- Body copy: Sniglet

You can download the fonts on this page:

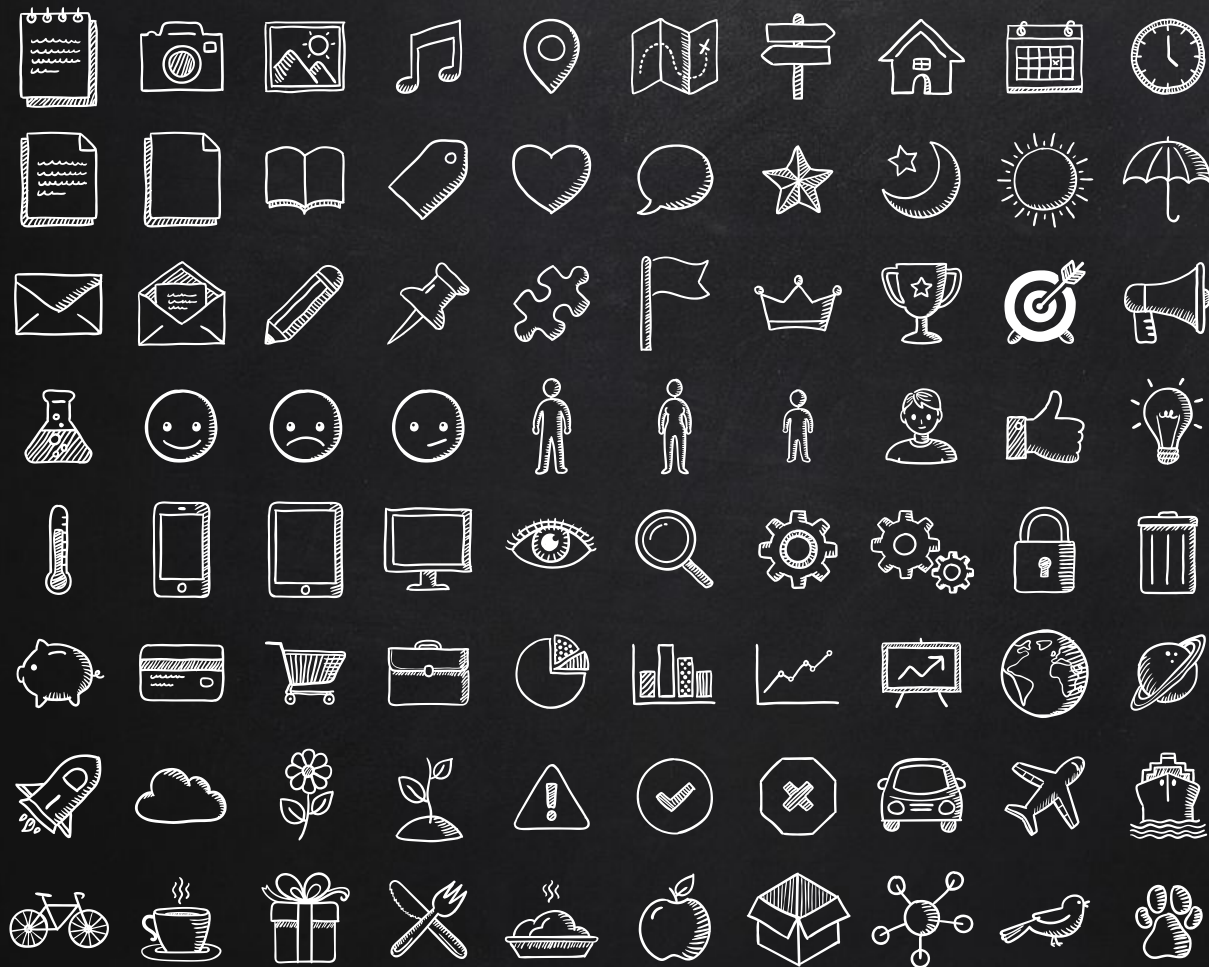
<https://www.google.com/fonts#UsePlace:use/Collection:Sniglet:400|Walter+Turncoat>

Click on the “arrow button” that appears on the top right



- White #FFFFFF

You don't need to keep this slide in your presentation. It's only here to serve you as a design guide if you need to create new slides or download the fonts to edit the presentation in PowerPoint®



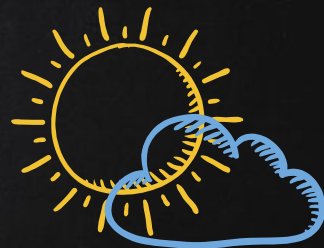
SlidesCarnival icons are editable shapes.

This means that you can:

- Resize them without losing quality.
- Change fill color and opacity.

Isn't that nice? :)

Examples:



# EXTRA GRAPHICS

