



TIP'S FOR WEB TESTING

WITH DANIIL SBOEV

For whom: first job seekers

After this session you will:

- Better understand daily QA activities
- Improve your resume with new skills
- Be able to present this knowledge on interview



About my self

Finished Portnov Online 2017 and worked as QA:

Broadway shows - small digital agency

Arteric - small digital agency

Pearson – big education company

New England Bank – medium bank

All jobs was manual.

I am enjoying with my job and salary 😊



Contents

Topic	Purposes	Time
Glossary	How to keep your knowledge	5
Bug tracker template	Easy and quick bug tracking template with Google Sheets	5
Cloud screenshots	How take a screenshot and benefits from cloud storage	5
Font Checker	How to quick check font parameters	5
Text comparison	Quick verification text content match to requirements	5
BrokenLinkCheck	Scan whole website for broken links	5
PageSpeed Insights	Quick performance test for web application	5
VirtualBox	Cross browser testing with virtual machines	5
BrowserStack	Cloud cross browser testing	5
Litmus	Cross platform testing for emails	5
	BREAK + Questions	10
Penetration Testing	How to hack web app with SQL and XSS injection	15
Proxy and VPN	How change IP for localization testing	10
Clean browser cache	When bug fixed, but we still reproduce it	5
Summary	Repeat all new knowledge and describe it for resume	5
	Questions + Wishes	10

Glossary

How to keep your knowledge?



OneNote, Excel, Trello

Quick verification text content match to requirements?

Bug Tracker Template:
<https://docs.google.com/spreadsheets/d/1RTCJZSEjrbXbKGabKkhuPwOt-ALSoDKjUi25DONcZPM/edit#gid=269511306>

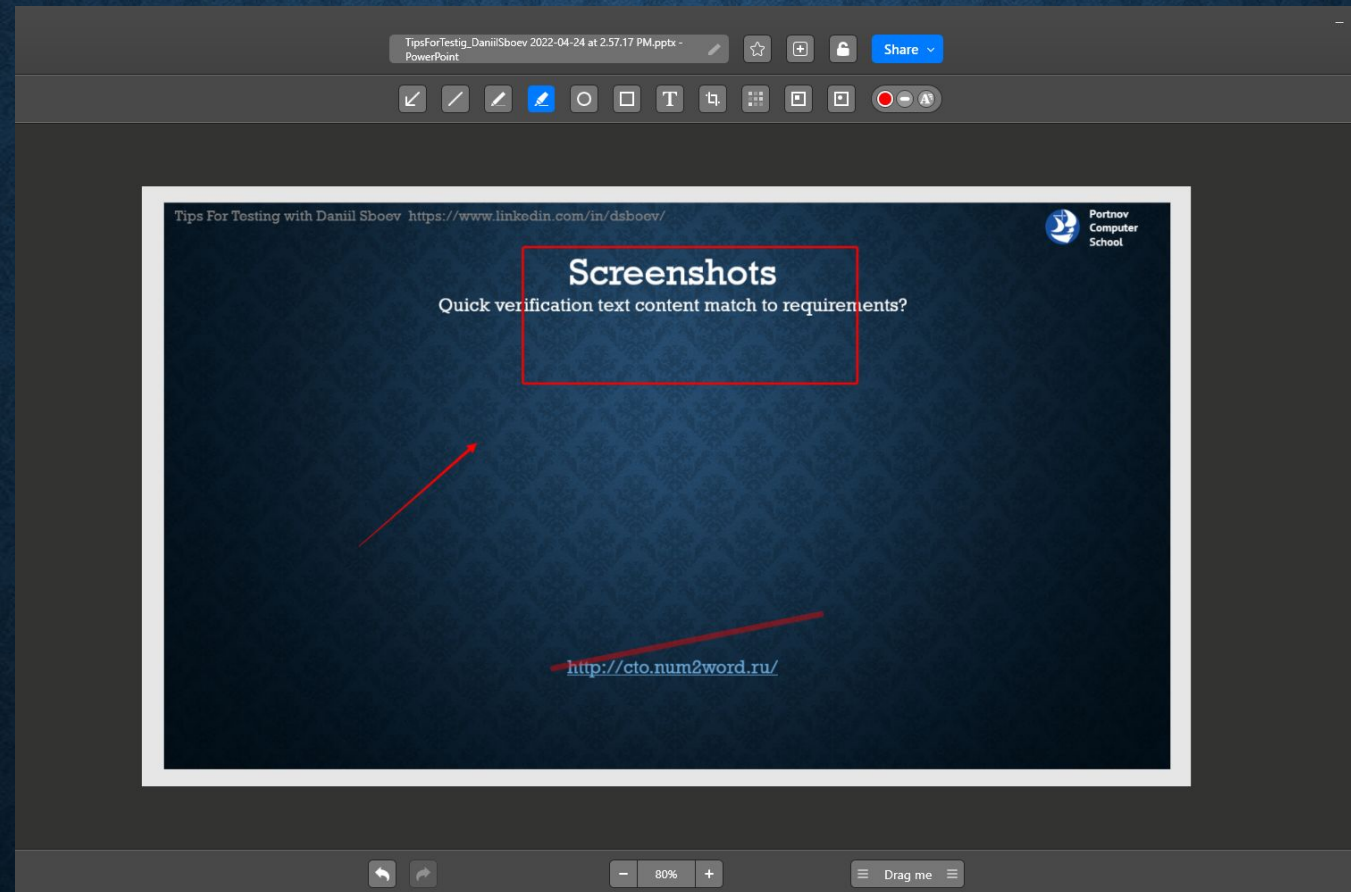


Screenshots

Windows: Shift+Win+S

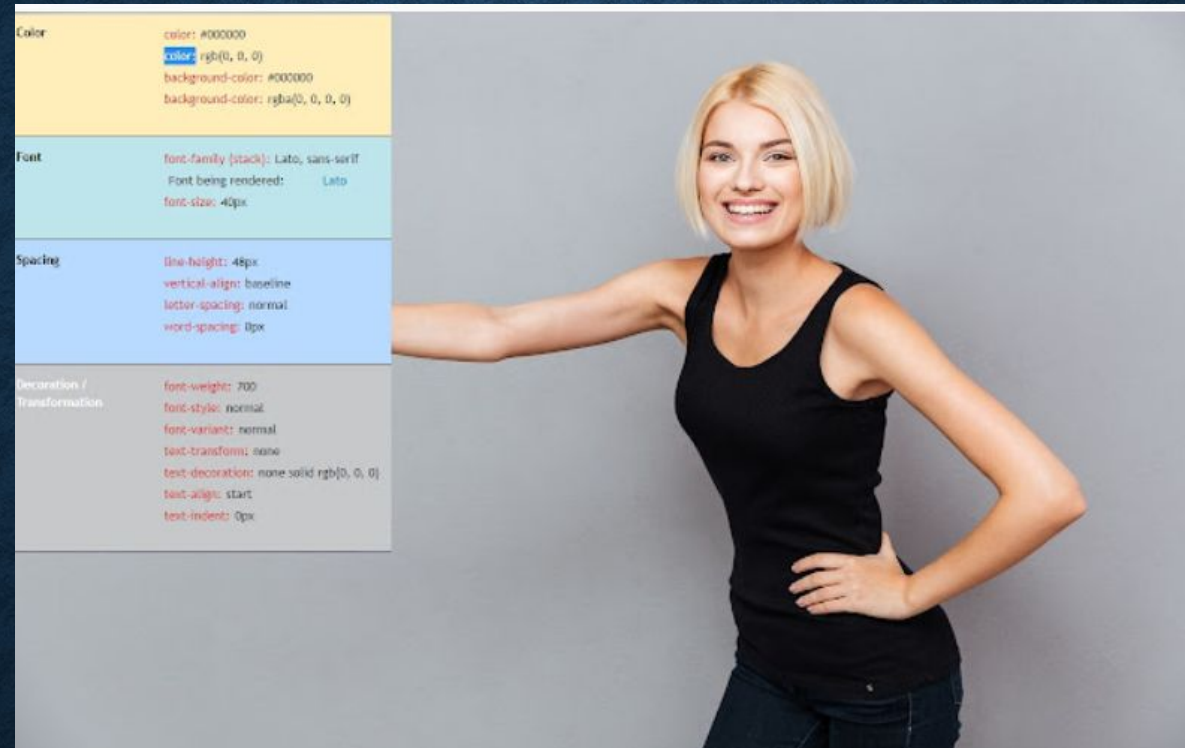
| MacOS: Shift+Cmd+4

- Quick Annotations
- Video recording
- Saved in cloud



Font checker

How to quick check font parameters



Font Finder:

<https://chrome.google.com/webstore/detail/font-finder/pkiokiaeahklmefmfpnnofmgfafaipdl?hl=en-US>



Text comparison

Quick verification text content match to requirements?

Compare text online

This site compares two texts and finds difference between them. The system compares signs. You can also easily customize text comparison result including colors.

☐ Remove ¶

☐ Uppercase/lowercase are the same

Default text color

To switch between differences in the text, press Enter or use the up / down buttons

First text :

Second text :

English is not their first language, people with zero programming skills or IT background — everybody can become a QA specialist and be ready to ace the interviews (and get a job) after completing our QA course e. Portnov Computer School is known as the pioneer in QA education. It is not only the oldest one in the U.S. (over 26 years) but is the only one backed by the U.S. Bureau for Private Postsecondary Education. Our graduates have an unheard-of success of 79 % placement rate. That's partly because we take care of our students like no other computer school. Every student goes through an internal internship and then can do one of several

background — everybody can become a QA specialist and be ready to ace the interviews (and get a job) after completing our QA course. Portnov Computer School is known as the pioneer in QA education. It is not only the oldest one in the U.S. (over 26 years) but is the only one backed by the U.S. Bureau for Private Postsecondary Education. Our graduates have an unheard-of success of 79 % placement rate. That's partly because we take care of our students like no other computer school. Every student goes through an internal internship and then can do one of several

Switch texts

Erase

Comparison timeout:

3

 second(s)

Text comparison result customization:

☒ Semantic cleanup

☐ Efficiency cleanup, edit cost:

4

☐ No cleanup

Compare

The texts are different! There are different signs in the texts.

Text comparison result:

=====

Imagine learning a new skill from scratch — no matter your current background¶ — and getting a job that has plenty of potential for advancement. That's QA. It¶ requires no special background and can be done in person or online. In fact, your¶ current background will probably help you be a great QA tester.¶ While many other jobs are getting outsourced, tech jobs are so much in demand¶ that companies can't hire fast enough.¶ Most programming jobs take years of education — but you can become a QA¶ specialist in just a few months. The industry is growing so fast that people are¶ often getting hired right out of our courses at \$35/hour. People who previously¶ worked minimum wage jobs in factories, grocery stores, etc., people for whom¶ English is not their first language, peo¶ ple with zero programming skills or IT¶ background — everybody can become a QA specialist and be ready to ace the¶ interviews (and get a job) after completing our QA course.¶

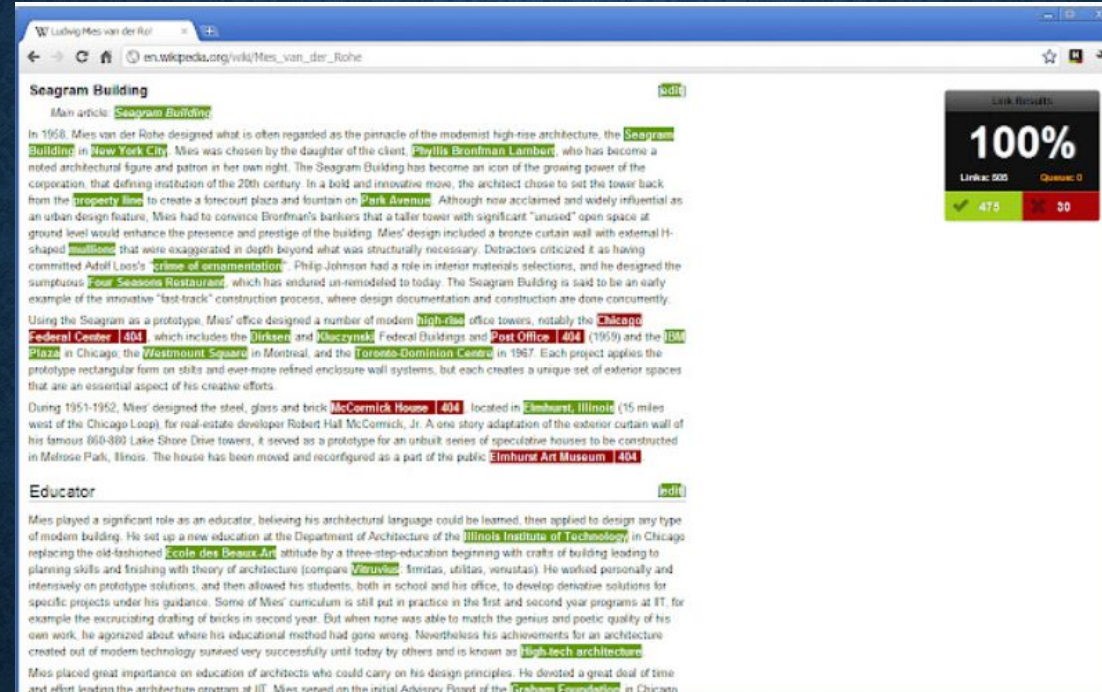
Down

Up

<http://cto.num2word.ru/>

BrokenLinkCheck

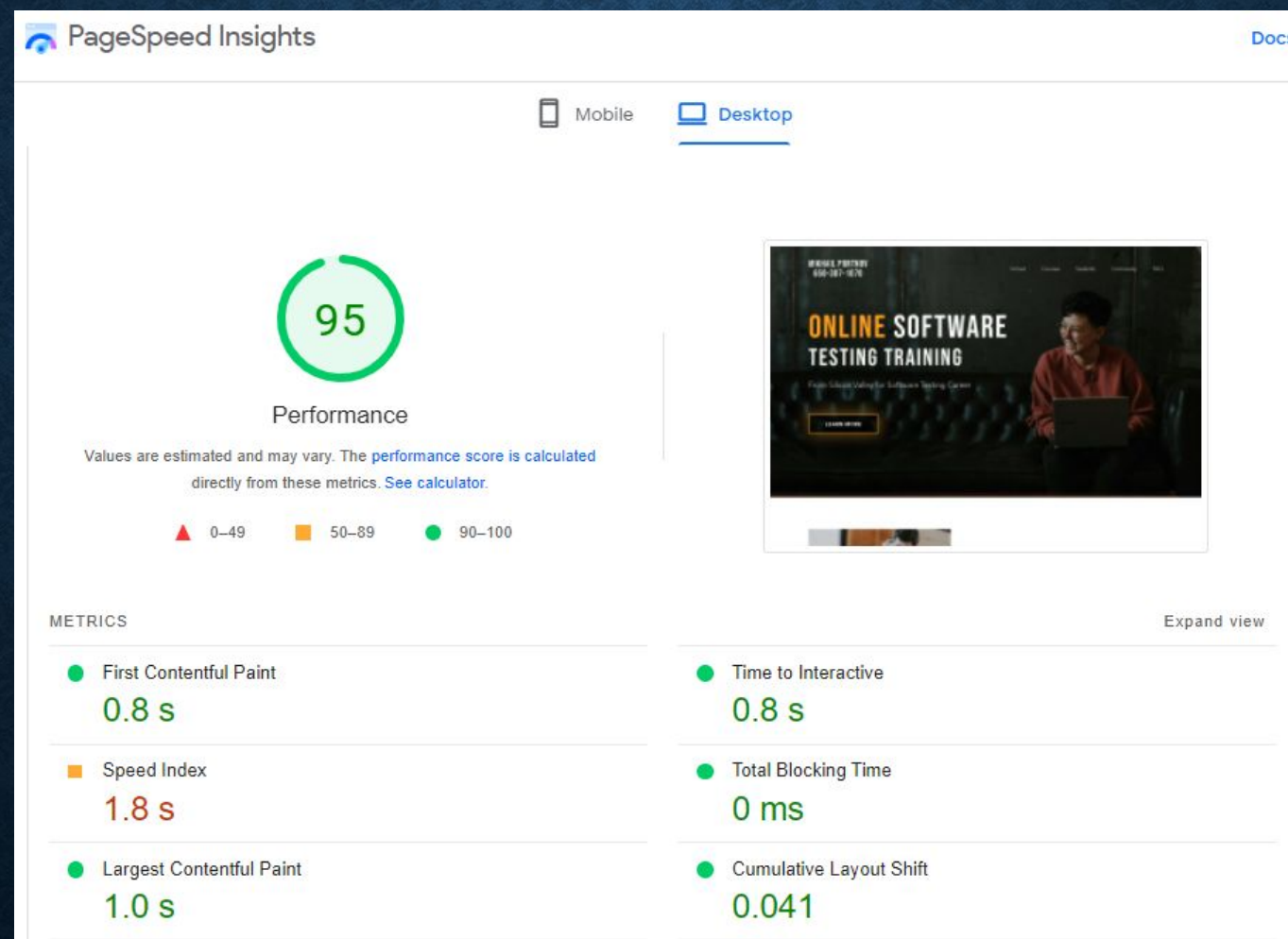
Scan whole web site for broken links



- Check My Links:
<https://chrome.google.com/webstore/detail/check-my-links/ojkcdipcgfaekbeaelapakgnjflglf?hl=en-US>
- <https://www.brokenlinkcheck.com/>
- <https://linktiger.com/>

PageSpeed Insights

Quick performance test for web application



<https://pagespeed.web.dev/>

Cross browser testing

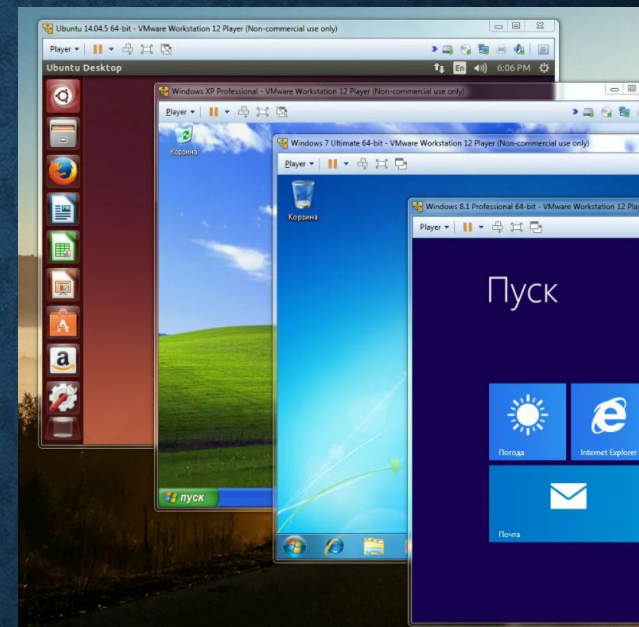
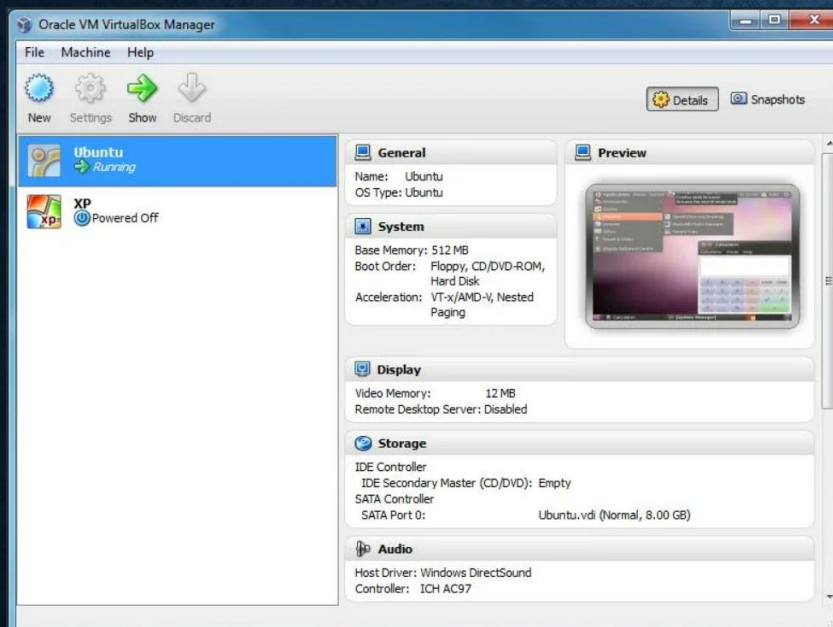
How to test web application in different browser versions?
For example you need test website in Chrome v96 and Chrome v95



Worst way: install and uninstall needed browser version every time.

Virtual machines

Virtual machines allow you to run an operating system in an app window on your desktop that behaves like a full, separate computer.




Better way for cross browsing: install different browser versions in different virtual machines.







BrowserStack

Cloud cross browser testing for desktop and mobile


 BrowserStack


Live Automate App Live App Automate Beta More ▾


 Invite my team Resources ▾ Account ▾





Quick Launch


 Android


 iOS


 Windows Phone


 Windows


 10

 8.1


 8


 7


 XP


 Mac


+


 16 Latest


 11 Latest

 56 Latest

 62 Latest

 48 Latest

 14.12 Latest

 5.1 Latest

15

57 Beta

63 Dev

49 Dev

14

55

61

47

54

60

46

53

59

45

52

58

44

51

57

43

50

56

42

49

55

41

48

54

40

16 more

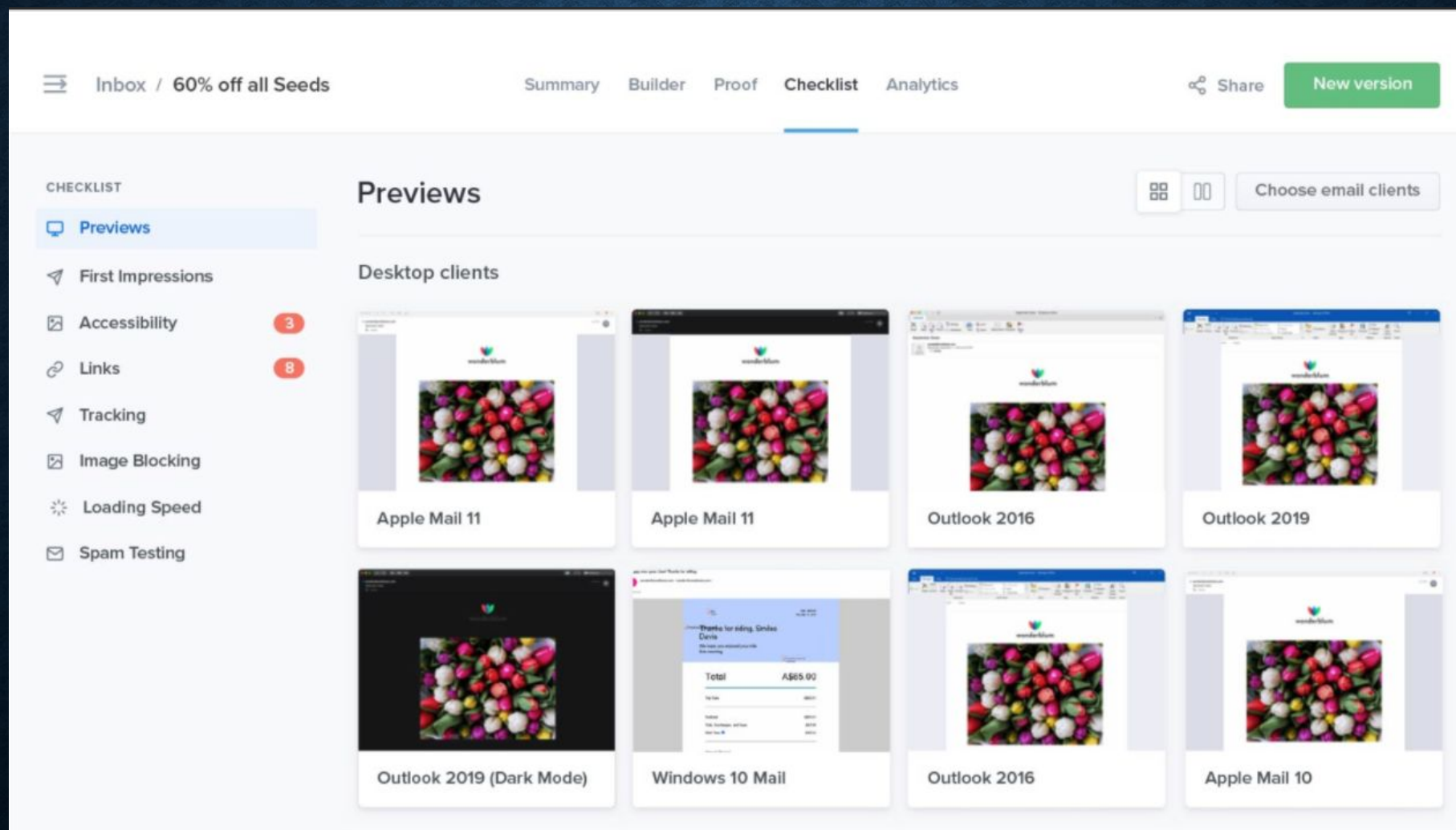
17 more

17 more

Drag a browser here to add to Quick Launch

Litmus

Cross platform testing for emails



The screenshot displays the Litmus web interface for testing email campaigns. At the top, a navigation bar includes a menu icon, the text "Inbox / 60% off all Seeds", and tabs for "Summary", "Builder", "Proof", "Checklist" (which is active), and "Analytics". On the right of the navigation bar are a "Share" icon and a green "New version" button.

On the left side, there is a "CHECKLIST" section with the following items: "Previews" (selected), "First Impressions", "Accessibility" (with a red circle containing the number 3), "Links" (with a red circle containing the number 8), "Tracking", "Image Blocking", "Loading Speed", and "Spam Testing".

The main content area is titled "Previews" and features a "Choose email clients" button. Below this, the "Desktop clients" section displays eight email preview cards arranged in two rows of four. Each card shows a thumbnail of the email as it appears in a specific client, with the client name labeled below the thumbnail.

Client	Client	Client	Client
Apple Mail 11	Apple Mail 11	Outlook 2016	Outlook 2019
Outlook 2019 (Dark Mode)	Windows 10 Mail	Outlook 2016	Apple Mail 10

BREAK 10 MINS

Ask your questions about passed topics in chat or grab a coffee.



Penetration Testing

How to hack web app with SQL injection

Safety engineer = try defense based on prediction 3a penetration

Penetration tester = legal hacker, verify is protection good enough

SQL injection might get access to whole data of database or even destroy it.
SQL injection is one of the most common web hacking techniques.



Browser <-> API <-> Logic <-> SQL query <-> Database
FILTER

Not allowed:] } ' " -- # > ? /* //



Penetration Testing

Example Step-1

Browser	Logic Server create SQL query
Iron Man	SELECT `title`,`release`,`character`,`genre`,`imdb` FROM `movies` WHERE title = `Iron Man`

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
Iron Man	2008	Tony Stark	action	Link

Penetration Testing

Example Step-2

Browser	Logic Server create SQL query
Iron Man`	<pre>SELECT `title`, `release`, `character`, `genre`, `imdb` FROM `movies` WHERE title = `Iron Man`</pre>

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '"' at line 1				



Penetration Testing

Example Step-3

Browser	Logic Server create SQL query
Iron Man''	SELECT `title`, `release`, `character`, `genre`, `imdb` FROM `movies` WHERE title = `Iron Man''`

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
No movies were found!				



Penetration Testing

Example Step-4

Browser	Logic Server create SQL query
Iron Man` OR 1=1--	<pre>SELECT `title`, `release`, `character`, `genre`, `imdb` FROM `movies` WHERE title = `Iron Man` OR 1=1--`</pre>

SQL Injection (GET/Search)

Search for a movie:

Search

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link



Penetration Testing

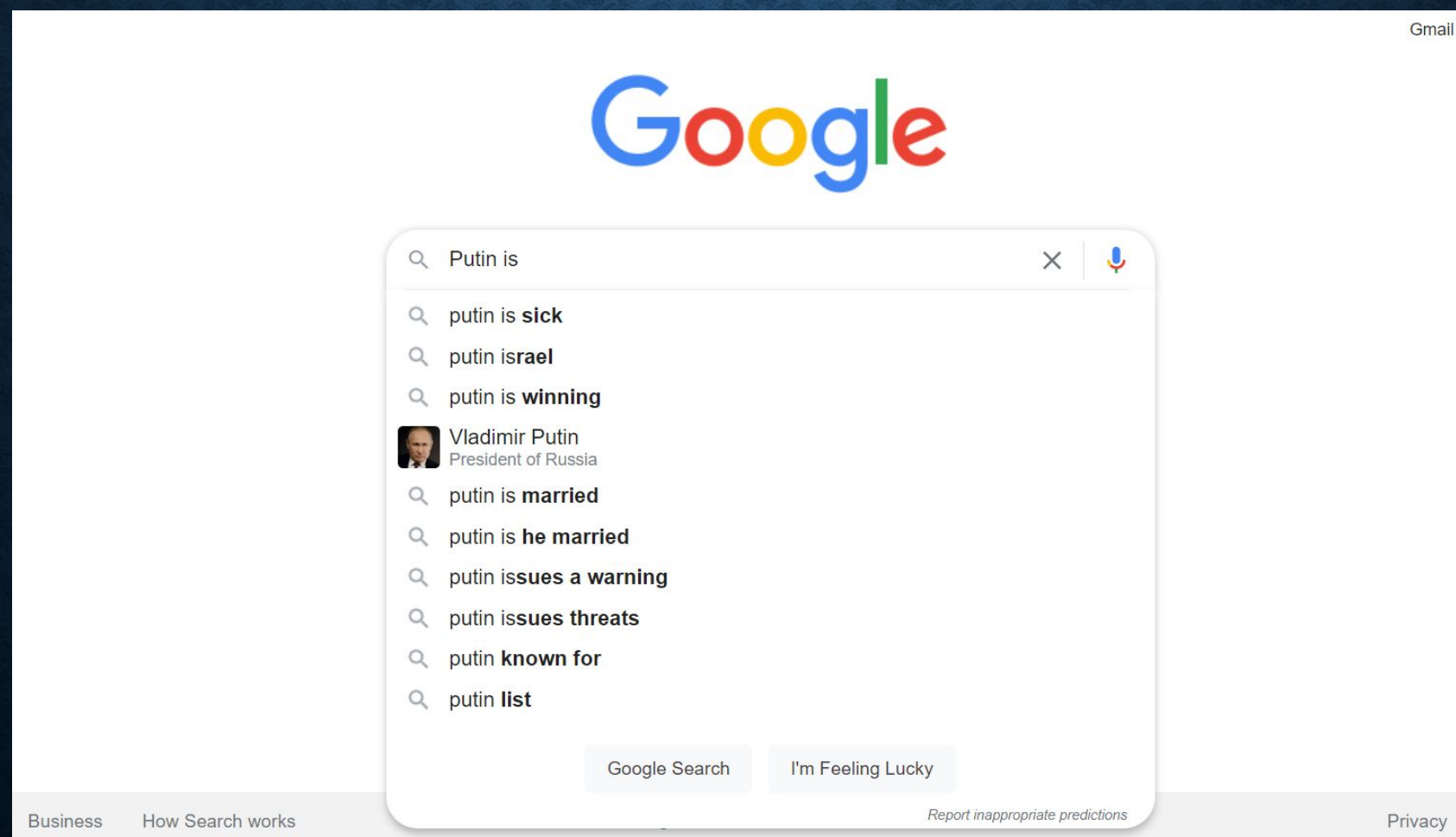
SQL injection - most common hacker attack:

Examples [\[edit \]](#)

- In February 2002, Jeremiah Jacks discovered that Guess.com was vulnerable to an SQL injection attack, permitting anyone able to construct a properly-crafted URL to pull down 200,000+ names, credit card numbers and expiration dates in the site's customer database.^[28]
- On November 1, 2005, a teenaged hacker used SQL injection to break into the site of a Taiwanese information security magazine from the Tech Target group and steal customers' information.^[29]
- On January 13, 2006, Russian computer criminals broke into a Rhode Island government website and allegedly stole credit card data from individuals who have done business online with state agencies.^[30]
- On March 29, 2006, a hacker discovered an SQL injection flaw in an official Indian government's tourism site.^[31]
- On June 29, 2007, a computer criminal defaced the Microsoft UK website using SQL injection.^{[32][33]} UK website *The Register* quoted a Microsoft spokesperson acknowledging the problem.
- On September 19, 2007 and January 26, 2009 the Turkish hacker group "m0sted" used SQL injection to exploit Microsoft's SQL Server to hack web servers belonging to McAlester Army Ammunition Plant and the US Army Corps of Engineers respectively.^[34]
- In January 2008, tens of thousands of PCs were infected by an automated SQL injection attack that exploited a vulnerability in application code that uses Microsoft SQL Server as the database store.^[35]
- In July 2008, Kaspersky's Malaysian site was hacked by the "m0sted" hacker group using SQL injection.
- On April 13, 2008, the Sexual and Violent Offender Registry of Oklahoma shut down its website for "routine maintenance" after being informed that 10,597 Social Security numbers belonging to sex offenders had been downloaded via an SQL injection attack^[36]
- In May 2008, a server farm inside China used automated queries to Google's search engine to identify SQL server websites which were vulnerable to the attack of an automated SQL injection tool.^{[35][37]}
- In 2008, at least April through August, a sweep of attacks began exploiting the SQL injection vulnerabilities of Microsoft's IIS web server and SQL Server database server. The attack does not require guessing the name of a table or column, and corrupts all text columns in all tables in a single request^[38] A HTML string that references a malware JavaScript file is appended to each value. When that database value is later displayed to a website visitor, the script attempts several approaches at gaining control over a visitor's system. The number of exploited web pages is estimated at 500,000.^[39]
- On August 17, 2009, the United States Department of Justice charged an American citizen, Albert Gonzalez, and two unnamed Russians with the theft of 130 million credit card numbers using an SQL injection attack. In reportedly "the biggest case of identity theft in American history", the man stole cards from a number of corporate victims after researching their payment processing systems. Among the companies hit were credit card processor Heartland Payment Systems, convenience store chain 7-Eleven, and supermarket chain Hannaford Brothers.^[40]
- In December 2009, an attacker breached a RockYou plaintext database containing the unencrypted usernames and passwords of about 32 million users using an SQL injection attack.^[41]
- In July 2010, a South American security researcher who goes by the handle "Ch Russo" obtained sensitive user information from popular BitTorrent site The Pirate Bay. He gained access to the site's administrative control panel and exploited an SQL injection vulnerability that enabled him to collect user account information, including IP addresses, MD5 password hashes and records of which torrents individual users have uploaded.^[42]
- From July 24 to 26, 2010, attackers from Japan and China used an SQL injection to gain access to customers' credit card data from Neo Beat, an Osaka-based company that runs a large online supermarket site. The attack also affected seven business partners including supermarket chains Izumiya Co, Maruetsu Inc, and Ryukyu Jusco Co. The theft of data affected a reported 12,191 customers. As of August 14, 2010 it was reported that there have been more than 300 cases of credit card information being used by third parties to purchase goods and services in China.
- On September 19 during the 2010 Swedish general election a voter attempted a code injection by hand writing SQL commands as part of a write-in vote.^[43]
- On November 8, 2010 the British Royal Navy website was compromised by a Romanian hacker named TinKode using SQL injection.^{[44][45]}
- On February 5, 2011 HBGary, a technology security firm, was broken into by LulzSec using an SQL injection in their CMS-driven website^[46]
- On March 27, 2011, www.mysql.com, the official homepage for MySQL, was compromised by a hacker using SQL blind injection^[47]
- On April 11, 2011, Barracuda Networks was compromised using an SQL injection flaw. Email addresses and usernames of employees were among the information obtained.^[48]
- Over a period of 4 hours on April 27, 2011, an automated SQL injection attack occurred on Broadband Reports website that was able to extract 8% of the username/password pairs: 8,000 random accounts of the 9,000 active and 90,000 old or inactive accounts.^{[49][50][51]}
- On June 1, 2011, "hacktivists" of the group LulzSec were accused of using SQLi to steal coupons, download keys, and passwords that were stored in plaintext on Sony's website, accessing the personal information of a million users.^[52]
- In June 2011, PBS was hacked by LulzSec, most likely through use of SQL injection; the full process used by hackers to execute SQL injections was described in this Imperva® blog.^[53]
- In May 2012, the website for Wurm Online, a massively multiplayer online game, was shut down from an SQL injection while the site was being updated.^[54]
- In July 2012 a hacker group was reported to have stolen 450,000 login credentials from Yahoo!. The logins were stored in plain text and were allegedly taken from a Yahoo subdomain, Yahoo! Voices. The group breached Yahoo's security by using a "union-based SQL injection technique".^{[55][56]}
- On October 1, 2012, a hacker group called "Team GhostShell" published the personal records of students, faculty, employees, and alumni from 53 universities including Harvard, Princeton, Stanford, Cornell, Johns Hopkins, and the University of Zurich on pastebin.com. The hackers claimed that they were trying to "raise awareness towards the changes made in today's education", bemoaning changing education laws in Europe and increases in tuition in the United States.^[57]
- In February 2013, a group of Maldivian hackers, hacked the website "UN-Maldives" using SQL Injection.
- On June 27, 2013, hacker group "RedHack" breached Istanbul Administration Site.^[58] They claimed that, they've been able to erase people's debts to water, gas, Internet, electricity, and telephone companies. Additionally, they published admin user name and password for other citizens to log in and clear their debts early morning. They announced the news from Twitter.^[59]
- On November 4, 2013, hacktivist group "RaptorSwag" allegedly compromised 71 Chinese government databases using an SQL injection attack on the Chinese Chamber of International Commerce. The leaked data was posted publicly in cooperation with Anonymous.^[60]
- On February 2, 2014, AVS TV had 40,000 accounts leaked by a hacking group called @deletesec^[61]
- On February 21, 2014, United Nations Internet Governance Forum had 3,215 account details leaked.^[62]
- On February 21, 2014, Hackers of a group called @deletesec hacked Spirol International after allegedly threatening to have the hackers arrested for reporting the security vulnerability. 70,000 user details were exposed over this conflict.^[63]
- On March 7, 2014, officials at Johns Hopkins University publicly announced that their Biomedical Engineering Servers had become victim to an SQL injection attack carried out by an Anonymous hacker named "Hooko" and aligned with hacktivist group "RaptorSwag". The hackers compromised personal details of 878 students and staff, posting a press release^[64] and the

Penetration Testing

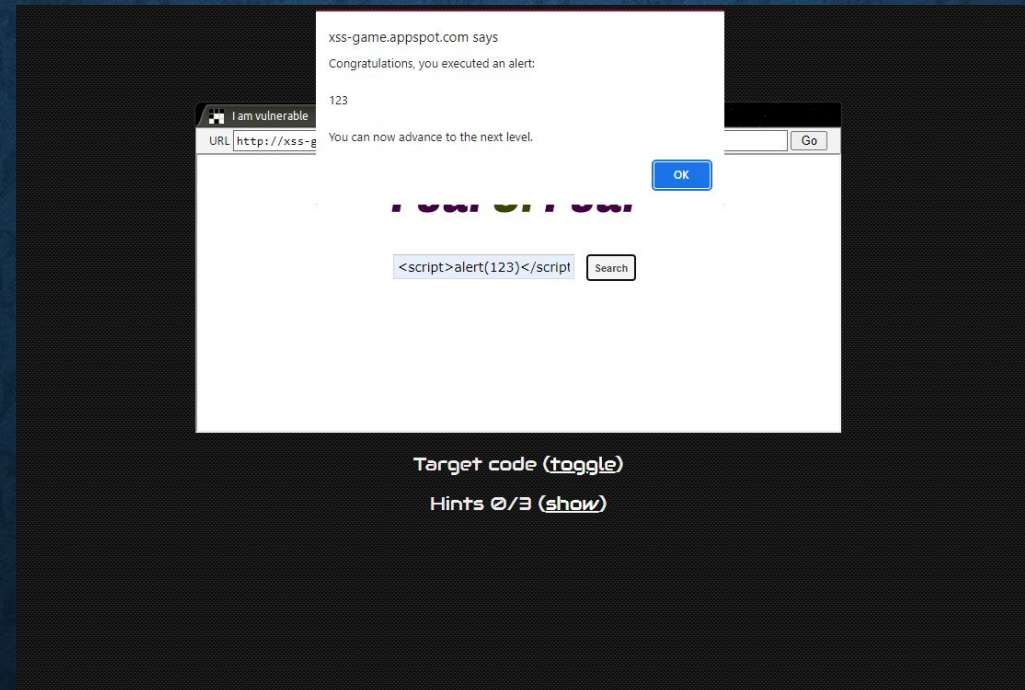
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites.



Penetration Testing

<http://xss-game.appspot.com/>

Template of Payload: `<script>alert(123)</script>`



XSS vulnerabilities have been present in around 50% of websites!



Penetration Testing

We are not penetration testers, but we can do simple tests.

For most testers keyword such as:

- Penetration testing
- SQL injection
- XSS protection
- Payload
- Even SAFETY

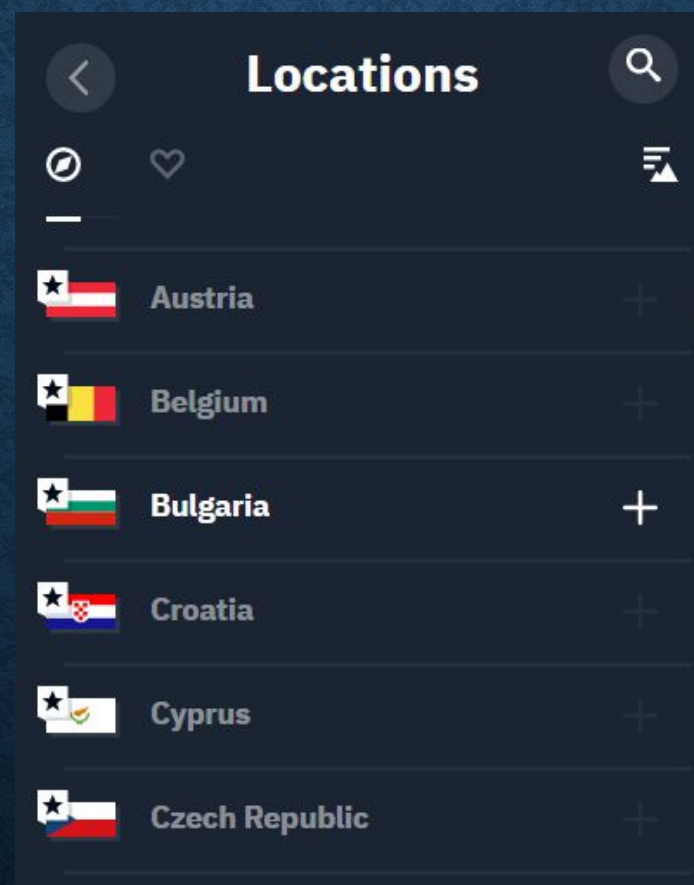
- its black box ;)

Pen testing – good for hobby, bug bounty – nice bonuses.

Never use penetration testing without permission, this is a criminal!

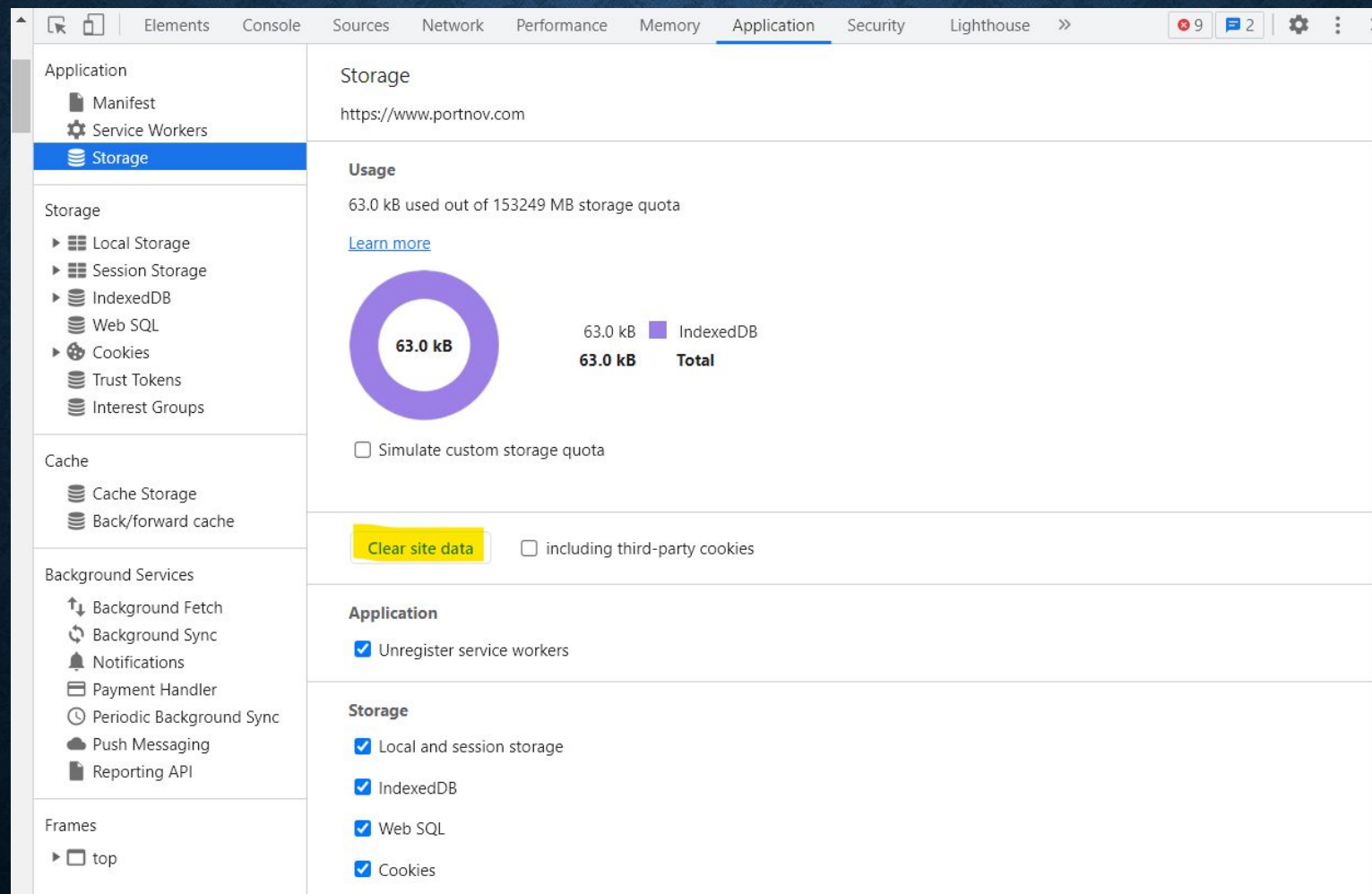
Localization Testing

Change IP with VPN for testing from different location.



Clean cache

Most common problem when when bug fixed, but we still reproduce it!



Application

- Manifest
- Service Workers
- Storage**

Storage

- Local Storage
- Session Storage
- IndexedDB
- Web SQL
- Cookies
- Trust Tokens
- Interest Groups

Cache

- Cache Storage
- Back/forward cache

Background Services

- Background Fetch
- Background Sync
- Notifications
- Payment Handler
- Periodic Background Sync
- Push Messaging
- Reporting API

Frames

- top

Storage

https://www.portnov.com

Usage

63.0 kB used out of 153249 MB storage quota

[Learn more](#)

63.0 kB IndexedDB

63.0 kB Total

☐ Simulate custom storage quota

Clear site data ☐ including third-party cookies

Application

- ☒ Unregister service workers

Storage

- ☒ Local and session storage
- ☒ IndexedDB
- ☒ Web SQL
- ☒ Cookies

Questions





Summary

Topic	Purposes
Glossary	How to keep your knowledge
Bug tracker template	Easy and quick bug tracking template with Google Sheets
Cloud screenshots	How take a screenshot and benefits from cloud storage
Font Checker	How to quick check font parameters
Text comparison	Quick verification text content match to requirements
BrokenLinkCheck	Scan whole web site for broken links
PageSpeed Insights	Quick performance test for web application
VirtualBox	Cross browser testing with virtual machines
BrowserStack	Cloud cross browser testing
Litmus	Cross platform testing for emails
Penetration Testing	How to hack web app with SQL and XSS injection
Proxy and VPN	How change IP for localization testing
Clean browser cache	When bug fixed, but we still reproduce it

Wishes



New job – not just salary or career. It's your happiness.

Don't stop – go to your Dream!