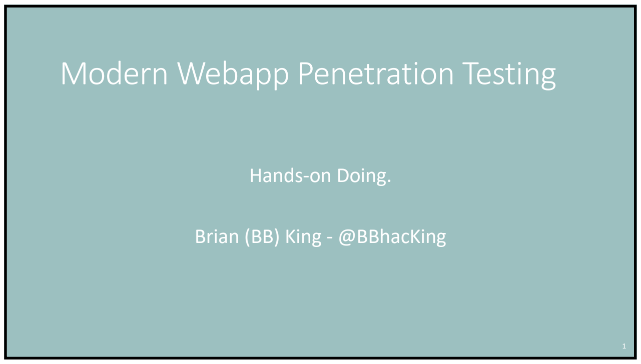


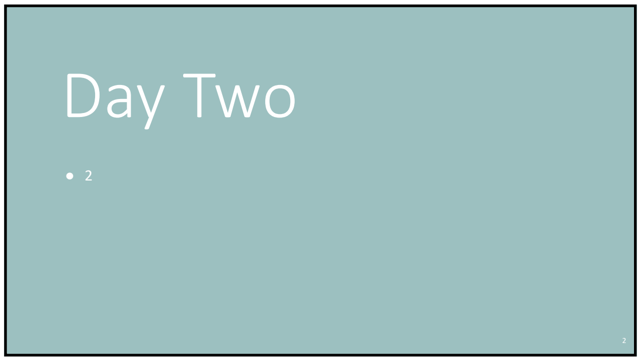
Modern Webapp Penetration Testing

Hands-on Doing.

Brian (BB) King - @BBhacKing

1

1

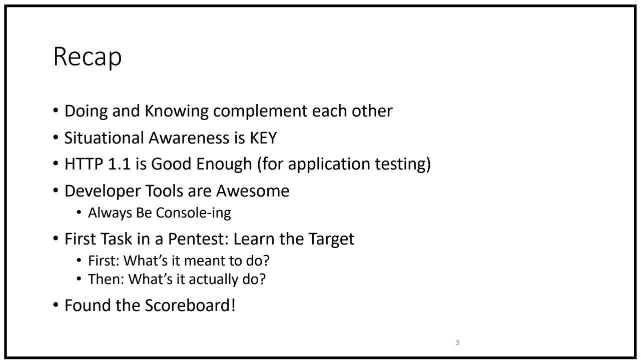


Day Two

- 2

2

2



Recap

- Doing and Knowing complement each other
- Situational Awareness is KEY
- HTTP 1.1 is Good Enough (for application testing)
- Developer Tools are Awesome
  - Always Be Console-ing
- First Task in a Pentest: Learn the Target
  - First: What's it meant to do?
  - Then: What's it actually do?
- Found the Scoreboard!

3

3

Today

- More “hidden content”
- Cross-user privacy invasions
- Defeating client-side controls
- Abusing faulty assumptions

4

4

Unlinked Content

Because “hidden” is too strong a word sometimes.

5

5

More About Unlinked Content

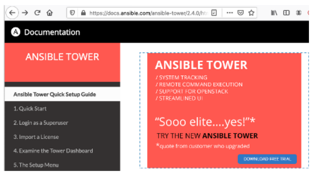
- Not always a conscious choice
- "Directory Indexing" is one example
  - Visit https://docs.ansible.com/ansible-tower/2.4.0/html/quickstart/
  - Now delete "quickstart/" from the end and reload the page
    - Seems harmless here, but.

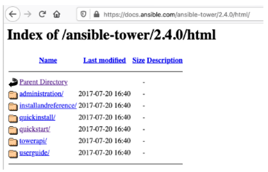
6

6

More About Unlinked Content

Normal Content **Directory Indexing Enabled**


https://docs.ansible.com/ansible-tower/2.4.0/htr


https://docs.ansible.com/ansible-tower/2.4.0/html/

```
Index of /ansible-tower/2.4.0/html

      Name             Last modified     Size Description

Parent Directory                          -
administration/      2017-07-20 16:40     -
installandreference/ 2017-07-20 16:40     -
quickinstall/        2017-07-20 16:40     -
quickstart/          2017-07-20 16:40     -
towerapi/            2017-07-20 16:40     -
userguide/           2017-07-20 16:40     -
```

7

7

HTTP and URLs

- Requests that end in a slash
  - What does it mean to request "a directory"?
- Default documents
  - index.html and friends
- Directory indexing
  - Instead of index.html
- Redirects
  - Visit https://www.blackhillsinfosec.com/training
    - ...there is no "/training" document – maybe it's a directory?
  - Notice you end up on https://www.blackhillsinfosec.com/training/
    - HTTP 301 "Moved Permanently"

8

8

Sometimes it *is* a Conscious Choice

- Don't show the "Admin" menu to non-admins
  - Actually omit it
  - Comment it out
  - Use CSS: "display: none"
  - Remove the href so visitors can't click it
- Remove the link to the WordPress login form
- Tell search engines not to index "hidden" things

9

9

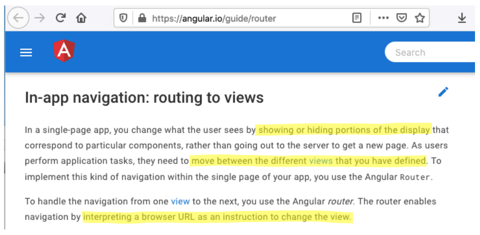
Modern Apps: Angular

- Angular JS Framework: https://angular.io/
- SPA: Single Page Application
- Web APIs to get data
- JS to render it
- JS to navigate among "views"
- Juice Shop uses Angular

10

10

Angular Routing



In-app navigation: routing to views

In a single-page app, you change what the user sees by showing or hiding portions of the display that correspond to particular components, rather than going out to the server to get a new page. As users perform application tasks, they need to move between the different views that you have defined. To implement this kind of navigation within the single page of your app, you use the Angular `Router`.

To handle the navigation from one view to the next, you use the Angular *router*. The router enables navigation by interpreting a browser URL as an instruction to change the view.

11

11

Angular Routing

- The main.js file is the (client-side) application
  - Routing rules for views
  - Client-side application logic
- Good place to find "secrets"

12

12

Angular Routing: Modern Mistakes

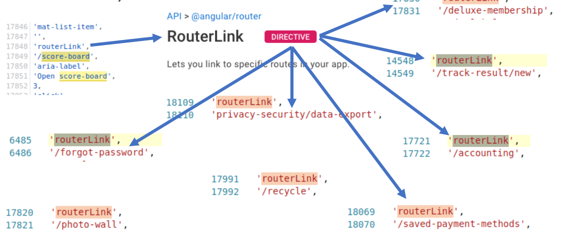
```
const appRoutes: Routes = [ {
   path: 'compose',
   component: ComposeMessageComponent,
   outlet: 'popup'
 }, {
   path: 'admin',
   loadChildren: () => import('./admin/admin.module').then(m => m.AdminModule),
   canLoad: [AuthGuard]
 }, {
   path: 'crisis-center',
   loadChildren: () => import('./crisis-center/crisis-center.module').then(m => m.CrisisCenterModule),
   data: { preload: true }
 },
. . .
];
```

13

13

Angular Routing in Juice Shop

All from main-es2015.js



```
'mat-list-item',
'',
'routerLink',
'/score-board',
'aria-label',
'Open score-board',
3,
```

```
'routerLink',
'/deluxe-membership',
```

```
'routerLink',
'/track-result/new',
```

```
'routerLink',
'privacy-security/data-export',
```

```
'routerLink',
'/forgot-password',
```

```
'routerLink',
'/accounting',
```

```
'routerLink',
'/recycle',
```

```
'routerLink',
'/photo-wall',
```

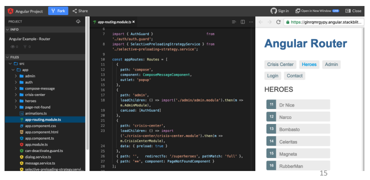
```
'routerLink',
'/saved-payment-methods',
```

14

14

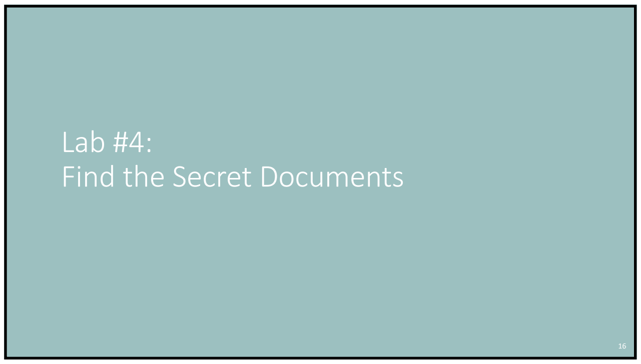
Live Angular Sample to Play In

- https://angular.io/guide/router
- Click "live example" to get to
- https://stackblitz.com/angular/glnrqmrgypy?file=src%2Fapp%2Fapp-routing.module.ts



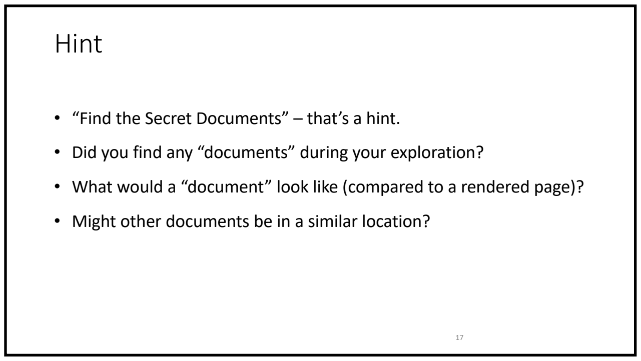
15

15


Lab #4:
Find the Secret Documents

16

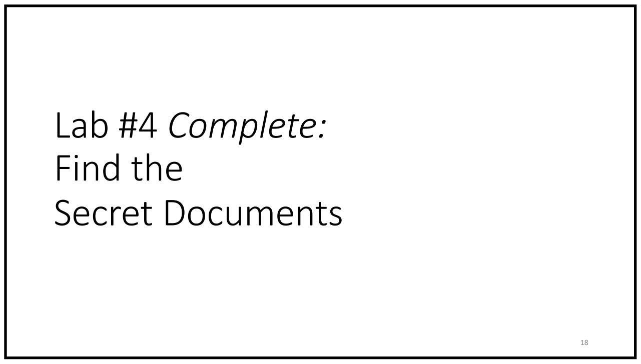
16


Hint

- “Find the Secret Documents” – that’s a hint.
- Did you find any “documents” during your exploration?
- What would a “document” look like (compared to a rendered page)?
- Might other documents be in a similar location?

17

17


Lab #4 *Complete:*
Find the
Secret Documents

18

18

What's Your Takeaway from the Lab?

19

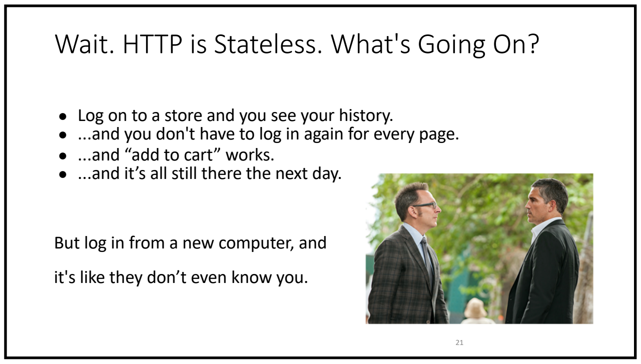
19

Maintaining State

With stateless protocols.

20

20



Wait. HTTP is Stateless. What's Going On?

- Log on to a store and you see your history.
- ...and you don't have to log in again for every page.
- ...and "add to cart" works.
- ...and it's all still there the next day.

But log in from a new computer, and

it's like they don't even know you.

21

21

State for the Stateless: Cookies

- Prove your identity, and you get a token (usually a cookie)
- So you don't have to prove your identity over and over

- Like a wristband at the water park.

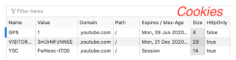
- Should be meaningless and unpredictable
- Should point to actual session state on the server

22

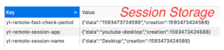
22

Stateless State

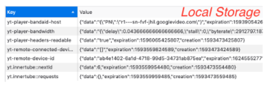
- Yes. Cookies. And also...
- Remember the "Storage" tab in Dev Tools?



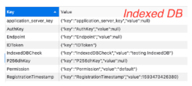
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly
GPS	1	.youtube.com	/	Mon, 29 Jun 2020...	4	false
VISITOR...	3m3rMFzNNSE	.youtube.com	/	Mon, 21 Dec 2020...	29	true
YSC	FwNoec-tTD0	.youtube.com	/	Session	14	true



Key	Value
yt-remote-fast-check-period	{"data":"1593473724588","creation":1593473424588}
yt-remote-session-app	{"data":"youtube-desktop","creation":1593473424588}
yt-remote-session-name	{"data":"Desktop","creation":1593473424588}



Key	Value
yt-player-bandaid-host	{"data":"{\"PN\":\"r1---sn-fvf-jhil.googlevideo.com\"}","expiration":1593905426
yt-player-bandwidth	{"data":"{\"delay\":0.043666666666666666,\"stall\":0,\"byterate\":2912797.18
yt-player-headers-readable	{"data":"true","expiration":1596065425807,"creation":1593473425807}
yt-remote-connected-devi...	{"data":"[]","expiration":1593559824589,"creation":1593473424589}
yt-remote-device-id	{"data":"ab4e1402-6a1d-4718-99d5-34731ab875ea","expiration":1624555277
yt.innertube::nextId	{"data":6,"expiration":1593559954480,"creation":1593473554480}
yt.innertube::requests	{"data":{},"expiration":1593559959485,"creation":1593473559485}



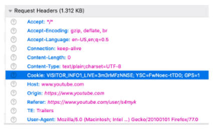
Key	Value
application_server_key	{"key":"application_server_key","value":null}
AuthKey	{"key":"AuthKey","value":null}
Endpoint	{"key":"Endpoint","value":null}
IDToken	{"key":"IDToken"}
IndexedDBCheck	{"key":"IndexedDBCheck","value":"testing IndexedDB"}
P256dhKey	{"key":"P256dhKey","value":null}
Permission	{"key":"Permission","value":"default"}
RegistrationTimestamp	{"key":"RegistrationTimestamp","value":1593473426380}

23

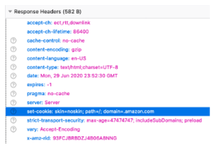
23

Browse with the Dev Tools Open

- Cookies are obvious: appearing in HTTP traffic *as cookies*.
  - HTTP Response Header "Set-Cookie" RFC 6265
    - Can also be set by client-side scripts, but even then...
  - HTTP Request Header "Cookie"



```
Request Headers (1.312 KB)
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Content-Length: 0
Content-Type: text/plain;charset=UTF-8
Cookie: VISITOR_INFO1_LIVE=3m3rMFzNNSE; YSC=FwNoec-tTD0; GPS=1
Host: www.youtube.com
Origin: https://www.youtube.com
Referer: https://www.youtube.com/user/s4myk
TE: Trailers
User-Agent: Mozilla/5.0 (Macintosh; Intel ...) Gecko/20100101 Firefox/77.0
```



```
Response Headers (582 B)
accept-ch: ect,rtt,downlink
accept-ch-lifetime: 86400
cache-control: no-cache
content-encoding: gzip
content-language: en-US
content-type: text/html;charset=UTF-8
date: Mon, 29 Jun 2020 23:52:30 GMT
expires: -1
pragma: no-cache
server: Server
set-cookie: skin=noskin; path=/; domain=.amazon.com
strict-transport-security: max-age=47474747; includeSubDomains; preload
vary: Accept-Encoding
x-amz-rid: 93FCJBRBDZJ4B06A8NNG
```

24

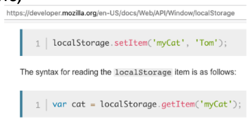
24

Local Storage

- Local Storage is NOT identified in HTTP Traffic
- Local Storage (or "DOM Storage") is part of the DOM
  - window.localStorage
  - window.sessionStorage

If you're only watching the HTTP traffic,

you will never know it's being used.



https://developer.mozilla.org/en-US/docs/Web/API/Window/localStorage

```
localStorage.setItem('myCat', 'Tom');
```

The syntax for reading the `localStorage` item is as follows:

```
var cat = localStorage.getItem('myCat');
```

25

25

DOM Storage vs Cookies

Similar uses, different details.

Property	Cookies	DOM Storage (Local Storage & Session Storage)
Access Restrictions	Same Origin Policy	Same Origin Policy
Lifetime	"session" or "persistent"	"session" or "persistent"
Size Limit	4KB per cookie, 20 cookies per origin.	5MB per origin
"Ambient Authority"	Yes (but diminishing)	No
Shows Up In...	HTTP Traffic, Dev Tools Storage	Developer Tools "Storage" pane

26

26

Lab #5:
View Someone Else's Shopping Cart

27

27

Don't Trust User Input

A lot of things are "user input"

What does the browser store?

Visit Google or Amazon: check "Storage" tab

28

28

Lab #5 Hint

View your own cart and look at the HTTP traffic

Check "Session Storage" in dev tools.

Done early? Look at these from Digi.Ninja:

- Client-Side Authentication: https://authlab.digi.ninja/ClientSide
- Permissions based on user-agent: https://authlab.digi.ninja/UserAgent
- IP Address based authentication: https://authlab.digi.ninja/Bypass

29

29

What's Your Takeaway from the Lab?

30

30

Insecure Direct Object Reference

- Integers may be the most obvious.
- Dates
- Usernames
- Email Addresses
- Filenames
- GUIDs
- Hash of filename, maybe?

31

31

“This Problem” or “This *Kind* of Problem”

Q: ”Why did the plane crash?”

A1: The pilot made a mistake.

OK, but people make mistakes. Why did this one happen?

A2: The pilot was tired.

OK, but people get tired. Why was the pilot flying while tired?

A3: This was the pilot’s fourth back-to-back 12-hour flight.

Oh! Let’s require that pilots get more rest between flights.

32

32

Insecure Direct Object Reference Root Cause Analysis:

Problem: Tester could see a cart without logging in as the cart owner.

What allowed that to happen?

Private item accessed by guessing its (small, predictable, integer) ID, based on knowledge of the tester’s own cart ID.

33

33

Insecure Direct Object Reference
Root Cause Analysis:

Problem: Tester could see a cart without logging in as the cart owner.

What allowed that to happen?

~~Private item accessed by guessing its (small, predictable, integer) ID, based on knowledge of the tester's own cart ID.~~

A private item was accessed by its ID without verifying that the requestor had the proper authority to see it.

34

34

The IDOR *Kind* of Problem

- Any "reference" that points to a non-public "thing"
- …where if you supply that reference, you get that thing.

- Not all "direct object references" are "insecure"
- Using a hard-to-guess reference…
  - adds difficulty, but
  - does not address the cause of the problem.

35

35

Lab #5 *Complete:* View Someone Else's Shopping Cart

36

36

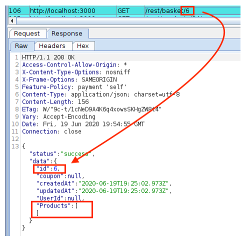
Web APIs

37

37

Web APIs are Not Very Different

- You just tested a REST API
- REST stands for something un-helpful.
  - It means "parameters in the path"
- POST data is not query-string format.
  - …that's the difference.



```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 156
ETag: W/"9c-t/1cNeD9A4K6q4xowsSKHgZW8t4"
Vary: Accept-Encoding
Date: Fri, 19 Jun 2020 19:54:55 GMT
Connection: close

{
  "status":"success",
  "data":{
    "id":6,
    "coupon":null,
    "createdAt":"2020-06-19T19:25:02.973Z",
    "updatedAt":"2020-06-19T19:25:02.973Z",
    "UserId":null,
    "Products":[
    ]
  }
}
```

38

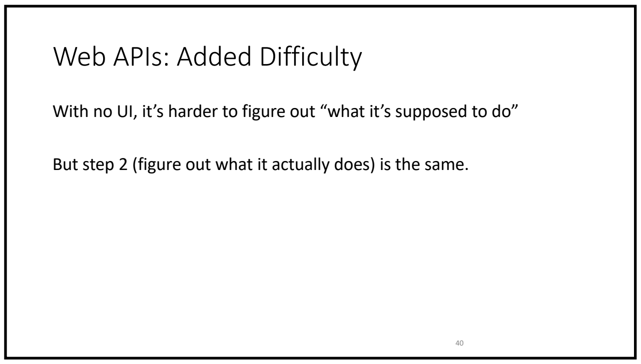
38

Web APIs are Not Very Different

- APIs: *designed* for non-browser clients
  - Can't learn by just clicking around
- Browser complexity is gone*
  - No parser, no renderer, no Javascript engine
  - No automatic cookie submission*
- Browser safeguards are gone*
  - No same-origin policy
  - No reliable "Origin" header
- XSS not possible* in Web APIs

39

39



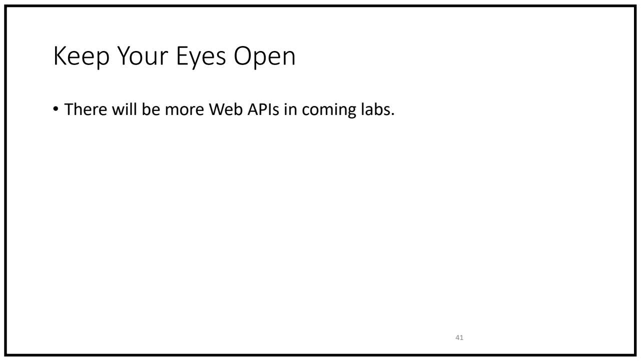
Web APIs: Added Difficulty

With no UI, it's harder to figure out "what it's supposed to do"

But step 2 (figure out what it actually does) is the same.

40

40



Keep Your Eyes Open

• There will be more Web APIs in coming labs.

41

41

Client-Side Controls

42

42

Client-Side Controls

A rule that is enforced on the client.

"On the client" == "In the browser"

Example: Input field lengths.

Example: Disabled or hidden form fields.

Example: multi-step sequences (e.g. shopping checkout)

43

43

Client-Side Controls: Good For...

Usability.

Save time: validate the form before submitting it

Help users avoid predictable errors

- Don't let them submit an incomplete form.
- Don't let them type 100 characters for a 32-character database field
- Make sure a phone number has enough digits, and no letters.

44

44

Client-Side Controls: Bad For...

Security.

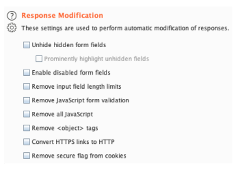
The user controls the client.

A browser is just one possible client.

Hostile users can easily bypass them

So can curious or bored ones...

Burp Suite "Response Modification" Checkboxes



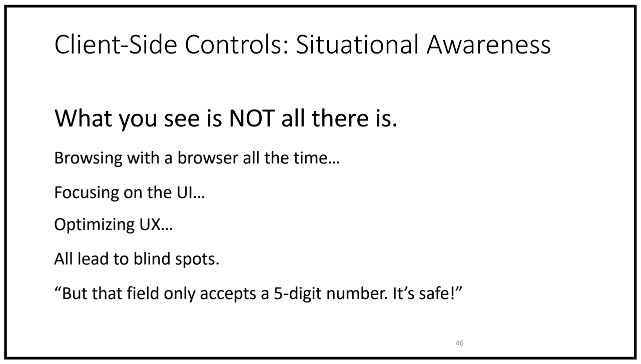
Response Modification

These settings are used to perform automatic modification of responses.

- ☐ Unhide hidden form fields
  - ☐ Prominently highlight unhidden fields
- ☐ Enable disabled form fields
- ☐ Remove input field length limits
- ☐ Remove JavaScript form validation
- ☐ Remove all JavaScript
- ☐ Remove <object> tags
- ☐ Convert HTTPS links to HTTP
- ☐ Remove secure flag from cookies

45

45



Client-Side Controls: Situational Awareness

What you see is NOT all there is.

Browsing with a browser all the time…

Focusing on the UI…

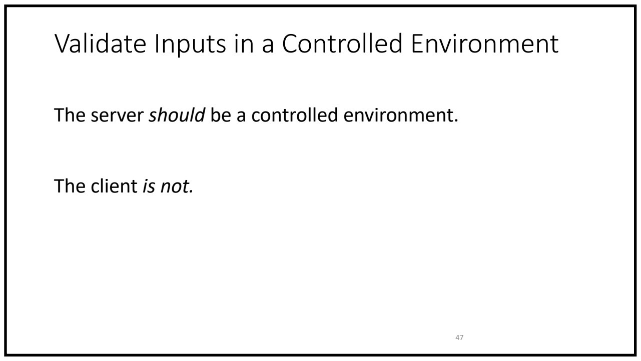
Optimizing UX…

All lead to blind spots.

“But that field only accepts a 5-digit number. It’s safe!”

46

46



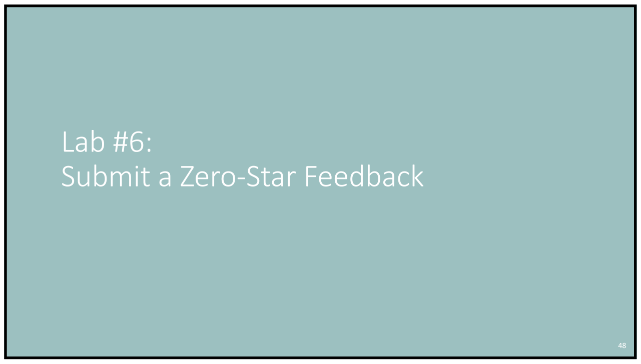
Validate Inputs in a Controlled Environment

The server *should* be a controlled environment.

The client *is not.*

47

47



Lab #6:
Submit a Zero-Star Feedback

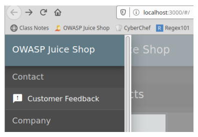
48

48

Lab #6 Hints

Customer Feedback
How does the Contact Us form behave?

(methodology: "what's it supposed to do?")



49

49

Lab #6 *Complete:* Submit a Zero-Star Feedback

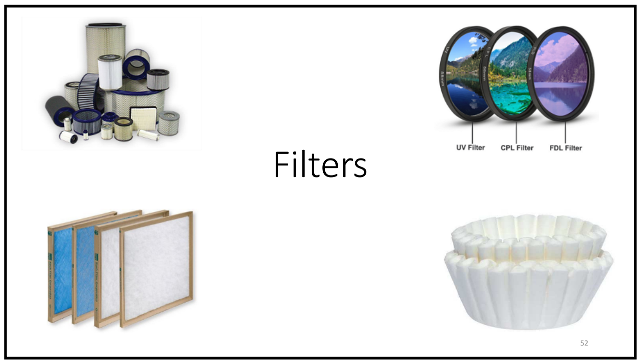
50

50

What's Your Takeaway from the Lab?

51

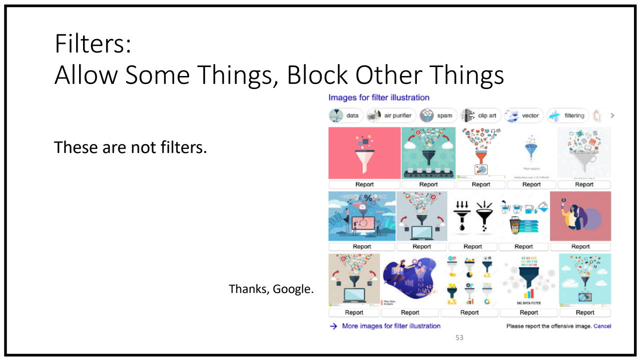
51



Filters

52

52



Filters:
Allow Some Things, Block Other Things

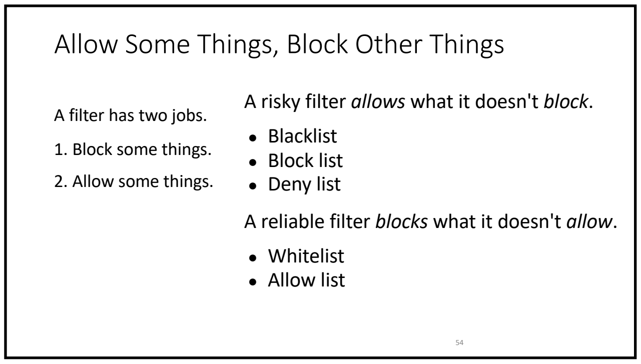
These are not filters.

Thanks, Google.

Images for filter illustration
data
air purifier
spam
clip art
vector
filtering
Report
More images for filter illustration
Please report the offensive image. Cancel

53

53



Allow Some Things, Block Other Things

A filter has two jobs.

1. Block some things.

2. Allow some things.

A risky filter *allows* what it doesn't *block*.

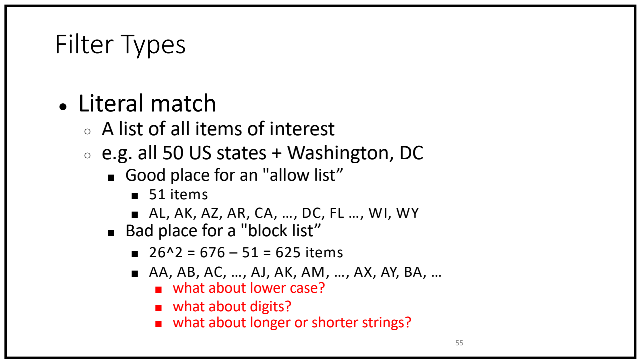
- Blacklist
- Block list
- Deny list

A reliable filter *blocks* what it doesn't *allow*.

- Whitelist
- Allow list

54

54

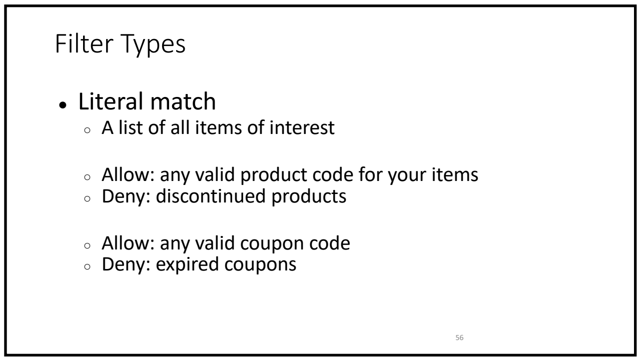


Filter Types

- Literal match
  - A list of all items of interest
  - e.g. all 50 US states + Washington, DC
    - Good place for an "allow list”
      - 51 items
      - AL, AK, AZ, AR, CA, …, DC, FL …, WI, WY
    - Bad place for a "block list”
      - 26^2 = 676 – 51 = 625 items
      - AA, AB, AC, …, AJ, AK, AM, …, AX, AY, BA, …
        - what about lower case?
        - what about digits?
        - what about longer or shorter strings?

55

55



Filter Types

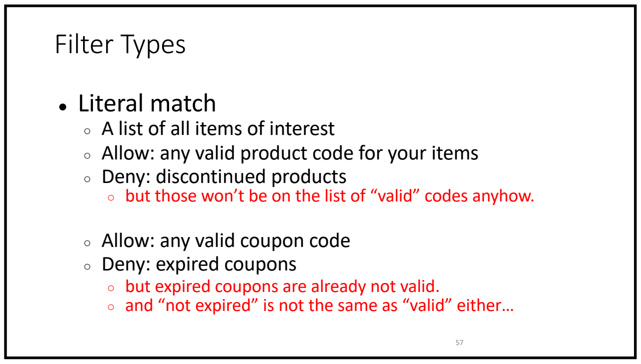
- Literal match
  - A list of all items of interest

  - Allow: any valid product code for your items
  - Deny: discontinued products

  - Allow: any valid coupon code
  - Deny: expired coupons

56

56



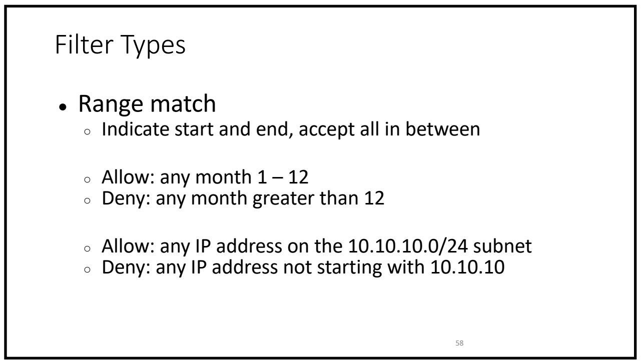
Filter Types

- Literal match
  - A list of all items of interest
  - Allow: any valid product code for your items
  - Deny: discontinued products
    - but those won’t be on the list of “valid” codes anyhow.

  - Allow: any valid coupon code
  - Deny: expired coupons
    - but expired coupons are already not valid.
    - and “not expired” is not the same as “valid” either…

57

57

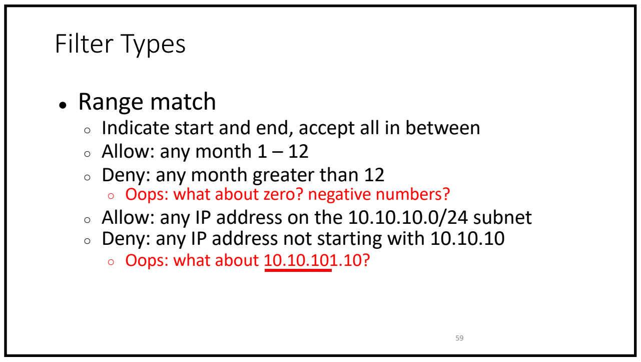


Filter Types

- Range match
  - Indicate start and end, accept all in between
  - Allow: any month 1 – 12
  - Deny: any month greater than 12
  - Allow: any IP address on the 10.10.10.0/24 subnet
  - Deny: any IP address not starting with 10.10.10

58

58

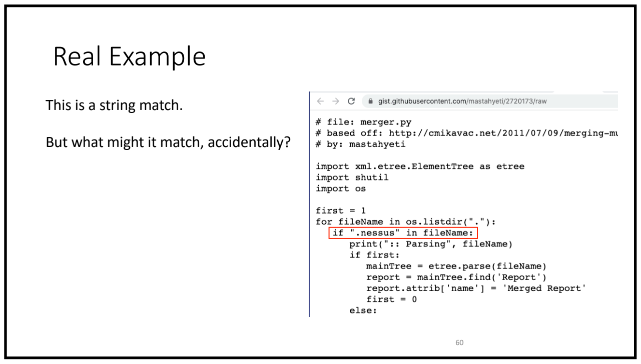


Filter Types

- Range match
  - Indicate start and end, accept all in between
  - Allow: any month 1 – 12
  - Deny: any month greater than 12
    - Oops: what about zero? negative numbers?
  - Allow: any IP address on the 10.10.10.0/24 subnet
  - Deny: any IP address not starting with 10.10.10
    - Oops: what about 10.10.101.10?

59

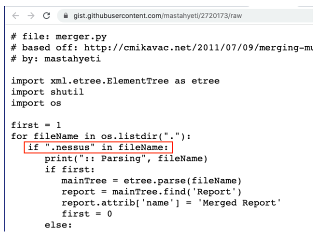
59



Real Example

This is a string match.

But what might it match, accidentally?

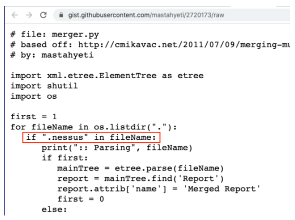


```
# file: merger.py
# based off: http://cmikavac.net/2011/07/09/merging-mu
# by: mastahyeti

import xml.etree.ElementTree as etree
import shutil
import os

first = 1
for fileName in os.listdir("."):
   if ".nessus" in fileName:
      print(":: Parsing", fileName)
      if first:
         mainTree = etree.parse(fileName)
         report = mainTree.find('Report')
         report.attrib['name'] = 'Merged Report'
         first = 0
      else:
```

60

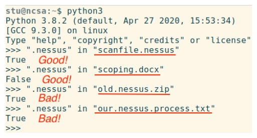
60

Real Example



gist.githubusercontent.com/mastahyeti/2720173/raw

```
# file: merger.py
# based off: http://cmikavac.net/2011/07/09/merging-mu
# by: mastahyeti

import xml.etree.ElementTree as etree
import shutil
import os

first = 1
for fileName in os.listdir("."):
   if ".nessus" in fileName:
      print(":: Parsing", fileName)
      if first:
         mainTree = etree.parse(fileName)
         report = mainTree.find('Report')
         report.attrib['name'] = 'Merged Report'
         first = 0
      else:
```



```
stu@ncsa:~$ python3
Python 3.8.2 (default, Apr 27 2020, 15:53:34)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license"
>>> ".nessus" in "scanfile.nessus"
True   Good!
>>> ".nessus" in "scoping.docx"
False   Good!
>>> ".nessus" in "old.nessus.zip"
True   Bad!
>>> ".nessus" in "our.nessus.process.txt"
True   Bad!
>>>
```

61

61

Filter Types

- Regular Expression match
  - A *pattern* that matches all items of interest
  - Uses literals, metacharacters, character classes, etc.

62

62

Regular Expressions

- Patterns for matching against.
- Any character usually matches itself.
  - meow matches a string that contains meow, like homeowner
- A dot is a metacharacter that matches any character
  - `ho.se` matches house and horse but not hose
- A caret anchors the pattern to the start of the string
  - `^ban` matches banana and bandana but not abandon
- A dollar anchors the pattern to the end of the string
  - `can$` matches pelican and can but not cannot

63

63

Regular Expressions

Character Classes in Regexes

\d means "any digit" and \D means "any non-digit"

[0-9] is the same as "any digit" and [^0-9] is the same as \D

\s means "whitespace" and \S means "non-whitespace"

different parsers define "whitespace" differently.

64

64

Regular Expressions

+ means "one or more of the preceding"

* means "zero or more of the preceding" (including the empty string!)

\ before a character means "treat this next one as literal"

Example: \+ matches a literal + and \. matches a literal dot.

65

65

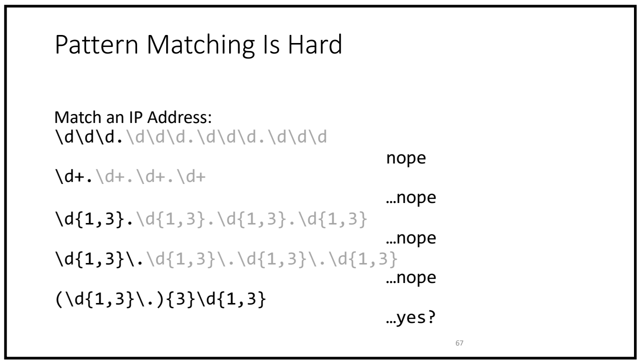
Regular Expressions

Some places to practice:

- https://regexr.com/
- https://regex101.com/
- CyberChef!

66

66



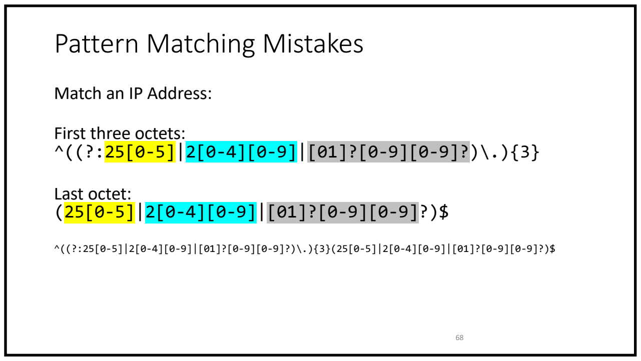
Pattern Matching Is Hard

Match an IP Address:

```
\d\d\d.\d\d\d.\d\d\d.\d\d\d
                                    nope
\d+.\d+.\d+.\d+
                                    …nope
\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}
                                    …nope
\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
                                    …nope
(\d{1,3}\.){3}\d{1,3}
                                    …yes?
```

67

67



Pattern Matching Mistakes

Match an IP Address:

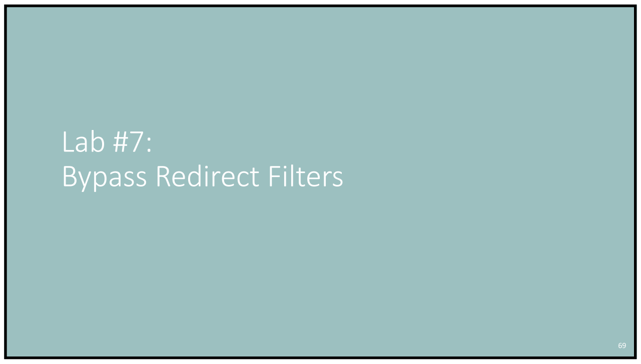
First three octets:
```
^((?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}
```

Last octet:
```
(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$
```

```
^((?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$
```

68

68



Lab #7:
Bypass Redirect Filters

69

69

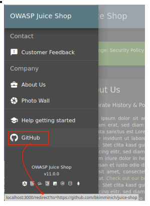
Redirect to Github

There's a redirect to Github in the left-side navigation.

Make it send you to a web server "that you control"

Or use Google.com or example.com to test.

Review URL structure if you get stuck.



localhost:3000/redirect?to=https://github.com/bkimminich/juice-shop

70

70

Lab #7 *Complete:* Bypass Redirect Filters

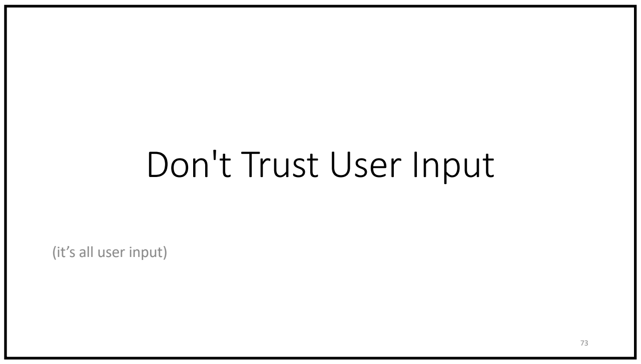
71

71

What's Your Takeaway from the Lab?

72

72

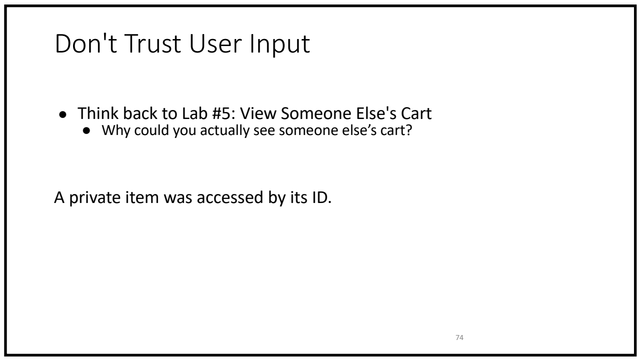


Don't Trust User Input

(it’s all user input)

73

73



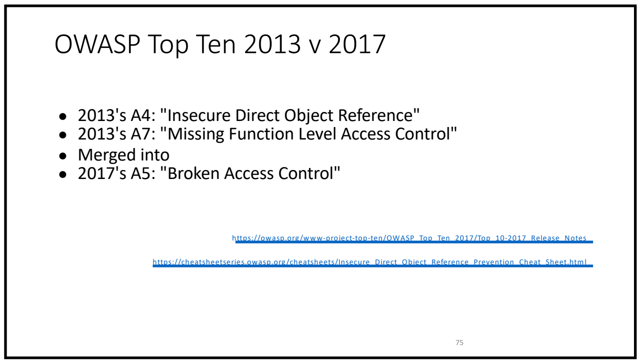
Don't Trust User Input

- Think back to Lab #5: View Someone Else's Cart
  - Why could you actually see someone else’s cart?

A private item was accessed by its ID.

74

74



OWASP Top Ten 2013 v 2017

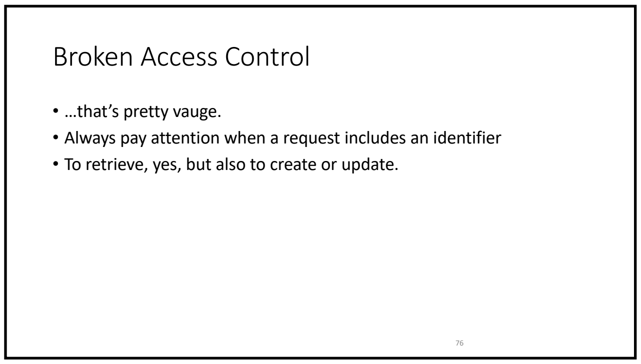
- 2013's A4: "Insecure Direct Object Reference"
- 2013's A7: "Missing Function Level Access Control"
- Merged into
- 2017's A5: "Broken Access Control"

https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_Release_Notes

https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

75

75



Broken Access Control

- …that’s pretty vauge.
- Always pay attention when a request includes an identifier
- To retrieve, yes, but also to create or update.

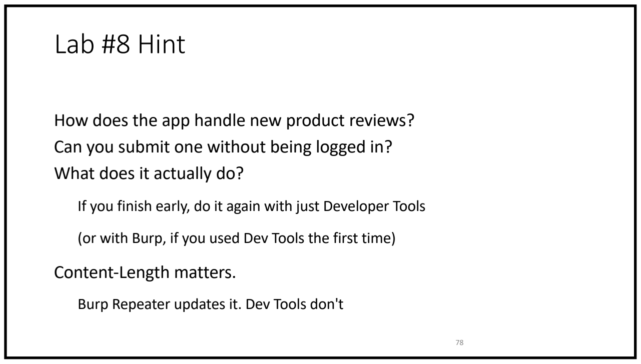
76

76

Lab #8:
Forge a Product Review

77

77



Lab #8 Hint

How does the app handle new product reviews?
Can you submit one without being logged in?
What does it actually do?

If you finish early, do it again with just Developer Tools

(or with Burp, if you used Dev Tools the first time)

Content-Length matters.

Burp Repeater updates it. Dev Tools don't

78

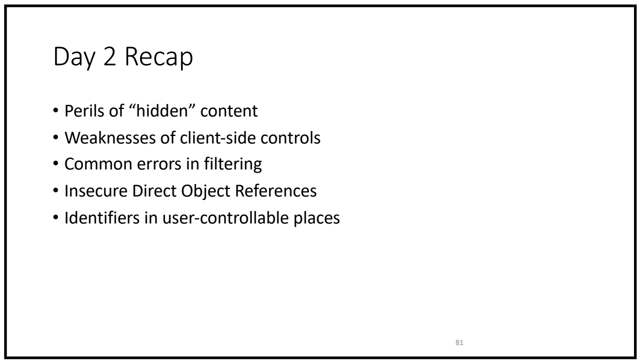
78

Lab #8 *Complete:* Forge a Product Review

79

What's Your Takeaway from the Lab?

80



Day 2 Recap

- Perils of “hidden” content
- Weaknesses of client-side controls
- Common errors in filtering
- Insecure Direct Object References
- Identifiers in user-controllable places

81