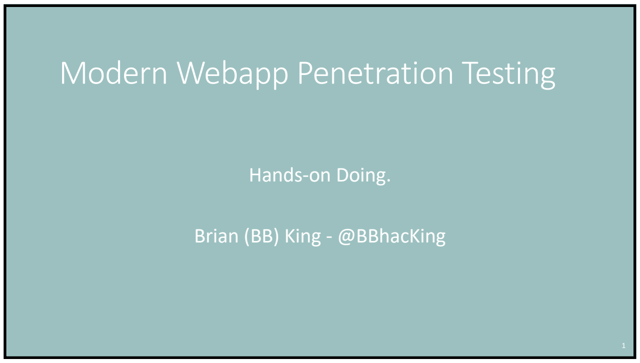


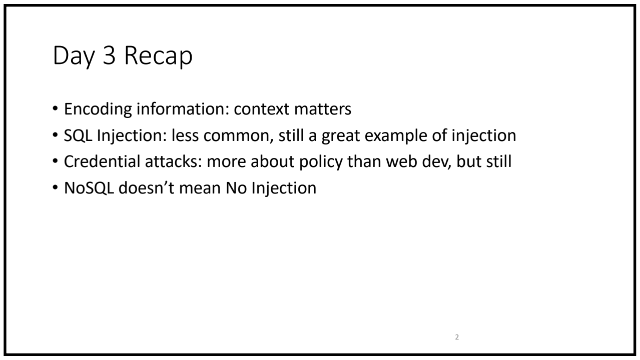
Modern Webapp Penetration Testing

Hands-on Doing.

Brian (BB) King - @BBhacKing

1

1



Day 3 Recap

- Encoding information: context matters
- SQL Injection: less common, still a great example of injection
- Credential attacks: more about policy than web dev, but still
- NoSQL doesn't mean No Injection

2

2

Reporting

Otherwise you're just playing around.

3

3

The Purpose, Again

- To Make Things Better
- To Make Computering Safer for Regular People

4

The Pentester's Role

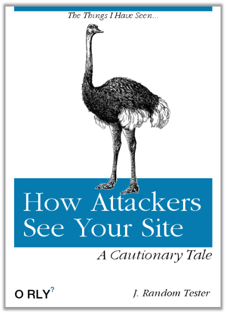
- Be the security "expert"
- Know how webapps work
- Know how and why wepapps fail
  - Security: just one of many worthwhile goals
  - Security: not true/false
- Communicate clearly
  - Some kind of report

5

The Report Tells A Story

- They know how it's meant to work.
- Tell them how it actually worked.

- Attacks that worked
- Attacks that failed



The Things I Have Seen...

How Attackers See Your Site

A Cautionary Tale

O RLY?

J. Random Tester

6

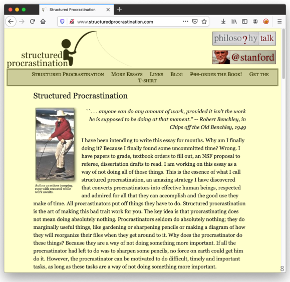
Screenshots Illustrate Your Story

- Illustrate, Don’t Decorate

7

7

Illustrate, Don’t Decorate


Structured Procrastination
www.structuredprocrastination.com
structured procrastination
philoso?hy talk
@stanford
Structured Procrastination More Essays Links Blog ~~Pre~~-order the Book! Get the T-shirt

Structured Procrastination

``. . . anyone can do any amount of work, provided it isn't the work he is supposed to be doing at that moment." -- Robert Benchley, in Chips off the Old Benchley, 1949

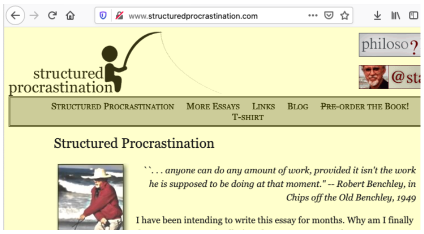
Author practices jumping rope with seaweed while work awaits.

I have been intending to write this essay for months. Why am I finally doing it? Because I finally found some uncommitted time? Wrong. I have papers to grade, textbook orders to fill out, an NSF proposal to referee, dissertation drafts to read. I am working on this essay as a way of not doing all of those things. This is the essence of what I call structured procrastination, an amazing strategy I have discovered that converts procrastinators into effective human beings, respected and admired for all that they can accomplish and the good use they make of time. All procrastinators put off things they have to do. Structured procrastination is the art of making this bad trait work for you. The key idea is that procrastinating does not mean doing absolutely nothing. Procrastinators seldom do absolutely nothing; they do marginally useful things, like gardening or sharpening pencils or making a diagram of how they will reorganize their files when they get around to it. Why does the procrastinator do these things? Because they are a way of not doing something more important. If all the procrastinator had left to do was to sharpen some pencils, no force on earth could get him do it. However, the procrastinator can be motivated to do difficult, timely and important tasks, as long as these tasks are a way of not doing something more important.

8

8

Illustrate, Don’t Decorate


www.structuredprocrastination.com
structured procrastination
philoso?
@st
Structured Procrastination More Essays Links Blog ~~Pre~~-order the Book!
T-shirt

Structured Procrastination

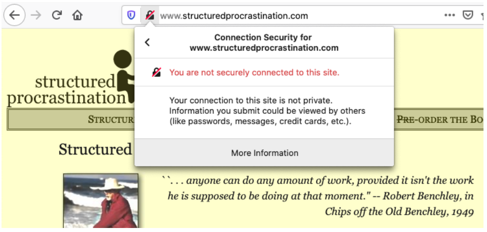
``. . . anyone can do any amount of work, provided it isn't the work he is supposed to be doing at that moment." -- Robert Benchley, in Chips off the Old Benchley, 1949

I have been intending to write this essay for months. Why am I finally

9

9

Illustrate, Don't Decorate


www.structuredprocrastination.com

Connection Security for www.structuredprocrastination.com

You are not securely connected to this site.

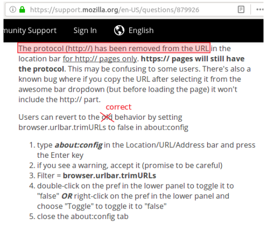
Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).

More Information

"`. . . anyone can do any amount of work, provided it isn't the work he is supposed to be doing at that moment." -- Robert Benchley, in Chips off the Old Benchley, 1949*

10

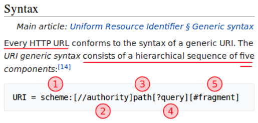
Coerce Your Browser Into Helping You


https://support.mozilla.org/en-US/questions/879926

The protocol (http://) has been removed from the URL in the location bar for http:// pages only. **https:// pages will still have the protocol**. This may be confusing to some users. There's also a known bug where if you copy the URL after selecting it from the awesome bar dropdown (but before loading the page) it won't include the http:// part.

Users can revert to the ~~old~~ correct behavior by setting browser.urlbar.trimURLs to false in about:config

1. type ***about:config*** in the Location/URL/Address bar and press the Enter key
2. if you see a warning, accept it (promise to be careful)
3. Filter = **browser.urlbar.trimURLs**
4. double-click on the pref in the lower panel to toggle it to "false" ***OR*** right-click on the pref in the lower panel and choose "Toggle" to toggle it to "false"
5. close the about:config tab


Syntax

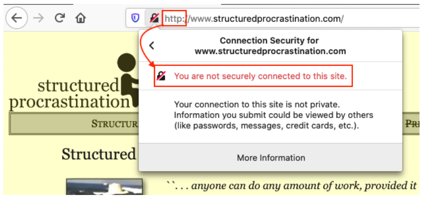
Main article: Uniform Resource Identifier § Generic syntax

Every HTTP URL conforms to the syntax of a generic URI. The *URI generic syntax* consists of a hierarchical sequence of five *components*:[14]

```
URI = scheme:[//authority]path[?query][#fragment]
```

11

Illustrate, Don't Decorate


http://www.structuredprocrastination.com/

Connection Security for www.structuredprocrastination.com

You are not securely connected to this site.

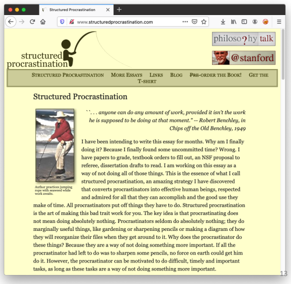
Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).

More Information

"`. . . anyone can do any amount of work, provided it*

12

Illustrate, Don't Decorate


Structured Procrastination
www.structuredprocrastination.com
philoso?hy talk
@stanford
structured procrastination
Structured Procrastination
More Essays
Links
Blog
~~Pre-~~order the Book!
Get the T-shirt

Structured Procrastination

``. . . anyone can do any amount of work, provided it isn't the work he is supposed to be doing at that moment." -- Robert Benchley, in Chips off the Old Benchley, 1949

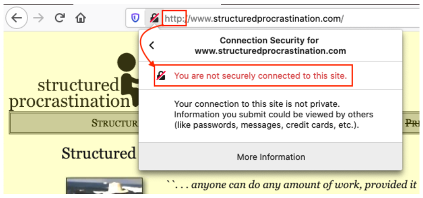
Author practices jumping rope with seaweed while work awaits.

I have been intending to write this essay for months. Why am I finally doing it? Because I finally found some uncommitted time? Wrong. I have papers to grade, textbook orders to fill out, an NSF proposal to referee, dissertation drafts to read. I am working on this essay as a way of not doing all of those things. This is the essence of what I call structured procrastination, an amazing strategy I have discovered that converts procrastinators into effective human beings, respected and admired for all that they can accomplish and the good use they make of time. All procrastinators put off things they have to do. Structured procrastination is the art of making this bad trait work for you. The key idea is that procrastinating does not mean doing absolutely nothing. Procrastinators seldom do absolutely nothing; they do marginally useful things, like gardening or sharpening pencils or making a diagram of how they will reorganize their files when they get around to it. Why does the procrastinator do these things? Because they are a way of not doing something more important. If all the procrastinator had left to do was to sharpen some pencils, no force on earth could get him do it. However, the procrastinator can be motivated to do difficult, timely and important tasks, as long as these tasks are a way of not doing something more important.

13

13

Illustrate, Don't Decorate


http://www.structuredprocrastination.com/
structured procrastination
Structur
Pr
Structured
More Information

Connection Security for www.structuredprocrastination.com

You are not securely connected to this site.

Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.).

``. . . anyone can do any amount of work, provided it

14

14

A Good Screenshot Is

Helpful	AND	Clear
• Relevant		• Legible
• Adds Useful Information		• Directs Viewer's Attention
• *Accurate*	*AND*	• *Precise*

15

15

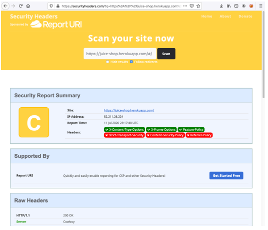
Screenshot Decisions

- Entire browser window, or …
- Plain screenshot, or …
- Text too small to read, or …
- Text too large to ignore
- Just the viewport, or …

- Crop to important part
- Something to direct attention
- Relevant text in image about the same size as body text around it.
- URL always included

16

Thoughtful Composition



Security Report Summary

C

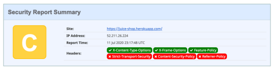
Site: https://juice-shop.herokuapp.com/
IP Address: 52.211.26.224
Report Time: 11 Jul 2020 23:17:48 UTC
Headers: ✓ X-Content-Type-Options ✓ X-Frame-Options ✓ Feature-Policy ✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ Referrer-Policy

Supported By

Report URI Quickly and easily enable reporting for CSP and other Security Headers!

Raw Headers

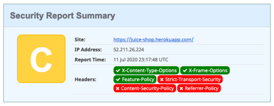
HTTP/1.1 200 OK
Server Cowboy



Security Report Summary

C

Site: https://juice-shop.herokuapp.com/
IP Address: 52.211.26.224
Report Time: 11 Jul 2020 23:17:48 UTC
Headers: ✓ X-Content-Type-Options ✓ X-Frame-Options ✓ Feature-Policy ✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ Referrer-Policy



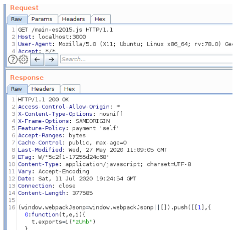
Security Report Summary

C

Site: https://juice-shop.herokuapp.com/
IP Address: 52.211.26.224
Report Time: 11 Jul 2020 23:17:48 UTC
Headers: ✓ X-Content-Type-Options ✓ X-Frame-Options ✓ Feature-Policy ✗ Strict-Transport-Security ✗ Content-Security-Policy ✗ Referrer-Policy

17

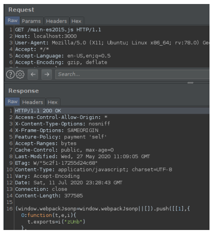
Thoughtful Contrast



```
GET /main-es2015.js HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:78.0) Ge
Accept: */*
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 27 May 2020 11:09:05 GMT
ETag: W/"5c2f1-17255d24c68"
Content-Type: application/javascript; charset=UTF-8
Vary: Accept-Encoding
Date: Sat, 11 Jul 2020 19:24:54 GMT
Connection: close
Content-Length: 377585

(window.webpackJsonp=window.webpackJsonp||[]).push([[1],{
  0:function(t,e,i){
    t.exports=i("zUnb")
  }
```



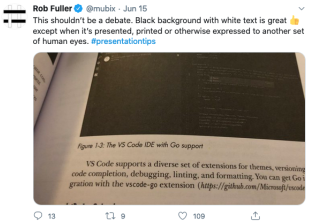
```
GET /main-es2015.js HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:78.0) Ge
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 27 May 2020 11:09:05 GMT
ETag: W/"5c2f1-17255d24c68"
Content-Type: application/javascript; charset=UTF-8
Vary: Accept-Encoding
Date: Sat, 11 Jul 2020 23:28:43 GMT
Connection: close
Content-Length: 377585

(window.webpackJsonp=window.webpackJsonp||[]).push([[1],{
  0:function(t,e,i){
    t.exports=i("zUnb")
  },
```

18

Thoughtful Contrast



Rob Fuller @mubix · Jun 15

This shouldn't be a debate. Black background with white text is great 👍 except when it's presented, printed or otherwise expressed to another set of human eyes. #presentationtips

Figure 1-3: The VS Code IDE with Go support

VS Code supports a diverse set of extensions for themes, versioning code completion, debugging, linting, and formatting. You can get Go i gration with the vscode-go extension (https://github.com/Microsoft/vscode

https://twitter.com/mubix/status/1272657499917815808

19

19

Thoughtful Words

- Explain clearly to "yourself, two years ago"
- Make it obvious how to reproduce the behavior
  - Include prerequisites
  - Include breadcrumbs or similar as needed
- Stick to the facts
  - Don't blame. Not even passively.

20

20

Attacking JSON Web Tokens

So much to practice in one small thing.

21

21

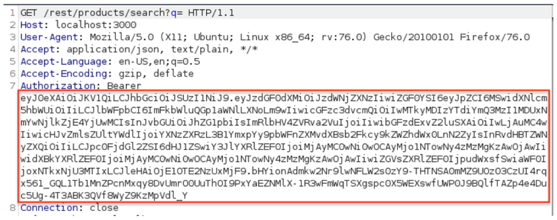
JSON Web Tokens Are…

These things:

```
eyJ0eXAiOiJKV1QiLA0KICJhbGciOiJIUzI1NiJ9.eyJp
c3MiOiJqb2UiLA0KICJleHAiOjEzMDA4MTkzODAsDQogI
mh0dHA6Ly9leGFtcGxlLmNvbS9pc19yb290Ijp0cnVlfQ
.dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk
```

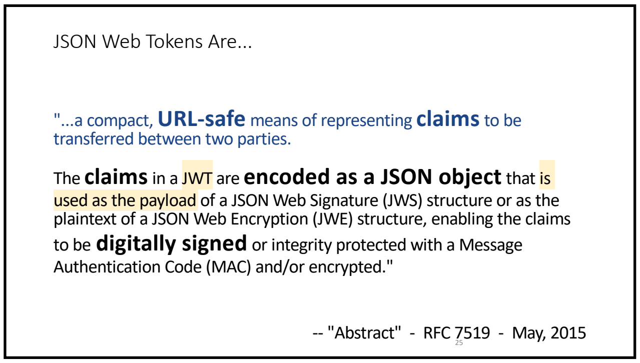
JSON Web Tokens Are…

These things…



```
GET /rest/products/search?q= HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm
5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxN
mYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4w
IiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWN
yZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMC0wNi0wOCAyMjo1NTowNy4zMzMgKzAwOjAwIi
widXBkYXRlZEF0IjoiMjAyMC0wNi0wOCAyMjo1NTowNy4zMzMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0I
joxNTkxNjU3MTIxLCJleHAiOjE1OTE2NzUxMjF9.bHYionAdmkw2Nr9lwNFLW2s0zY9-THTNSA0mMZ9U0z03CzUI4rq
x561_GQL1Tb1MnZPcnMxqy8DvUmrO0UuThOI9PxYaEZNMlX-1R3wFmWqTSXgspc0X5WEXswfUWP0J9BQlfTAZp4e4Du
c5Ug-4T3ABK3QVf8WyZ9KzMpVdl_Y
Connection: close
```

Not All Input Looks Like Input



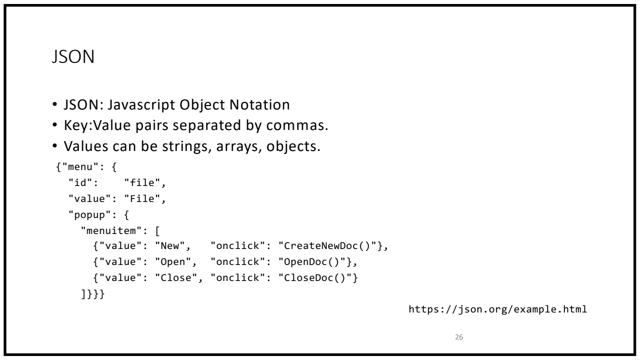
JSON Web Tokens Are...

"...a compact, **URL-safe** means of representing **claims** to be transferred between two parties.

The **claims** in a JWT are **encoded as a JSON object** that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be **digitally signed** or integrity protected with a Message Authentication Code (MAC) and/or encrypted."

-- "Abstract" - RFC 7519 - May, 2015

25



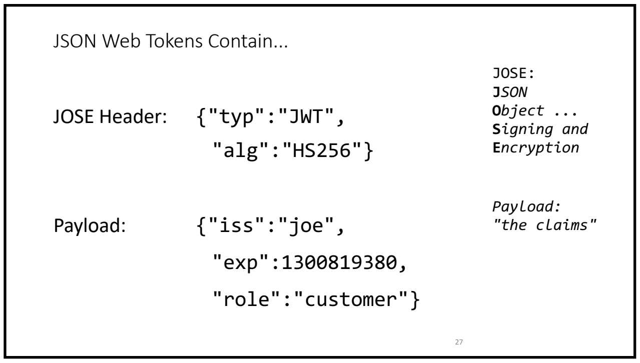
JSON

- JSON: Javascript Object Notation
- Key:Value pairs separated by commas.
- Values can be strings, arrays, objects.

```
{"menu": {
  "id":    "file",
  "value": "File",
  "popup": {
    "menuitem": [
      {"value": "New",   "onclick": "CreateNewDoc()"},
      {"value": "Open",  "onclick": "OpenDoc()"},
      {"value": "Close", "onclick": "CloseDoc()"}
    ]}}}
```

https://json.org/example.html

26



JSON Web Tokens Contain...

JOSE Header:

```
{"typ":"JWT",
  "alg":"HS256"}
```

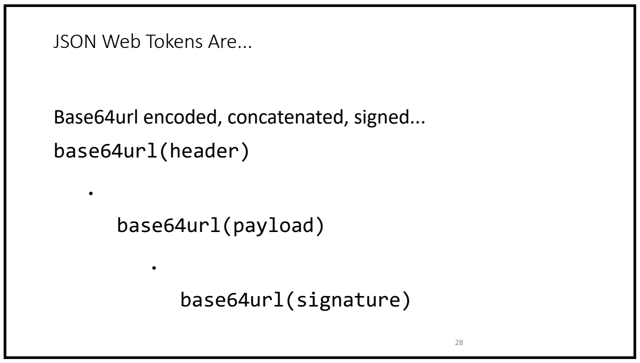
JOSE:
J*SON*
O*bject ...*
S*igning and*
E*ncryption*

Payload:

```
{"iss":"joe",
  "exp":1300819380,
  "role":"customer"}
```

Payload:
"the claims"

27

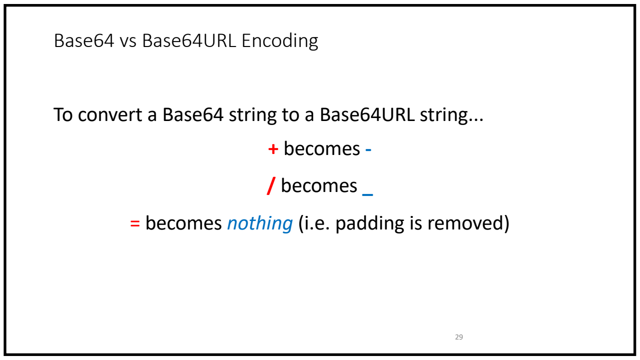


JSON Web Tokens Are...

Base64url encoded, concatenated, signed...

```
base64url(header)
    .
        base64url(payload)
            .
                base64url(signature)
```

28



Base64 vs Base64URL Encoding

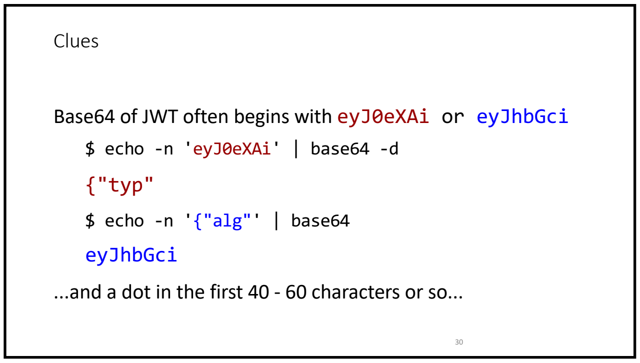
To convert a Base64 string to a Base64URL string...

+ becomes -

/ becomes _

= becomes *nothing* (i.e. padding is removed)

29



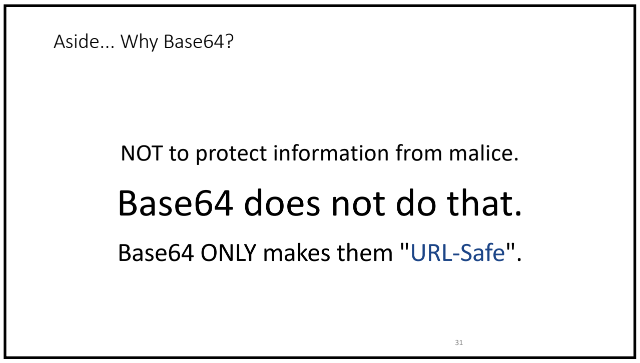
Clues

Base64 of JWT often begins with `eyJ0eXAi` or `eyJhbGci`

```
$ echo -n 'eyJ0eXAi' | base64 -d
{"typ"
$ echo -n '{"alg"' | base64
eyJhbGci
```

...and a dot in the first 40 - 60 characters or so...

30



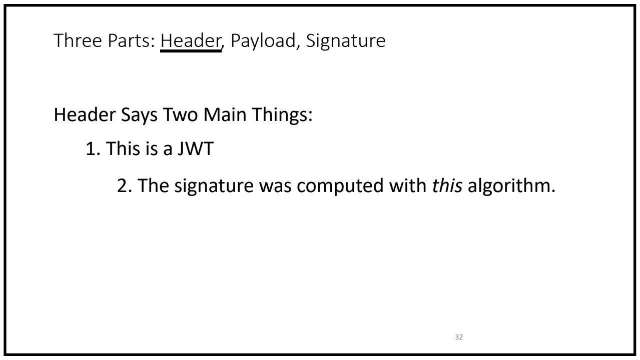
Aside... Why Base64?

NOT to protect information from malice.

Base64 does not do that.

Base64 ONLY makes them "URL-Safe".

31

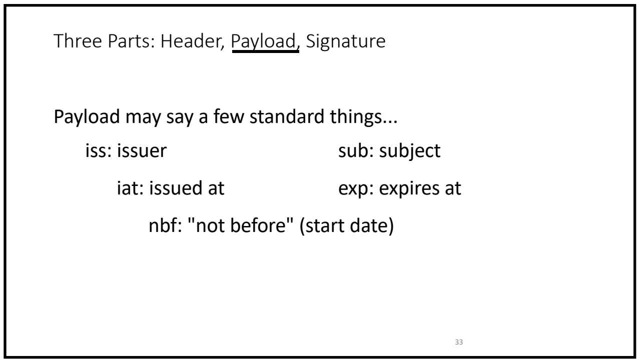


Three Parts: Header, Payload, Signature

Header Says Two Main Things:

1. This is a JWT
2. The signature was computed with *this* algorithm.

32



Three Parts: Header, Payload, Signature

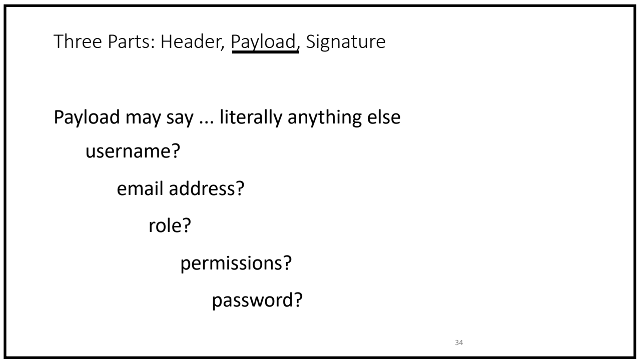
Payload may say a few standard things...

iss: issuer sub: subject

iat: issued at exp: expires at

nbf: "not before" (start date)

33



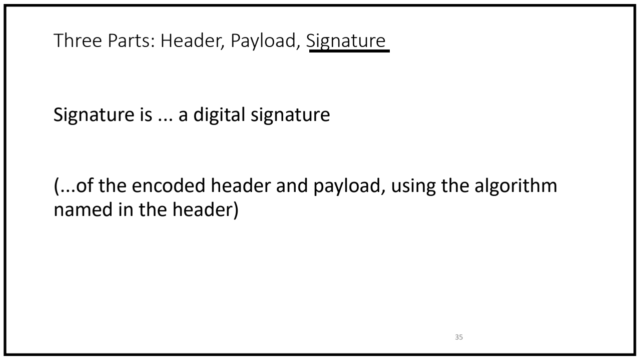
Three Parts: Header, Payload, Signature

Payload may say ... literally anything else

- username?
  - email address?
    - role?
      - permissions?
        - password?

34

34



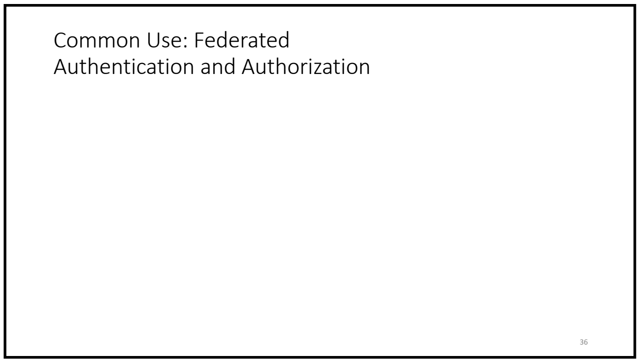
Three Parts: Header, Payload, Signature

Signature is ... a digital signature

(...of the encoded header and payload, using the algorithm named in the header)

35

35



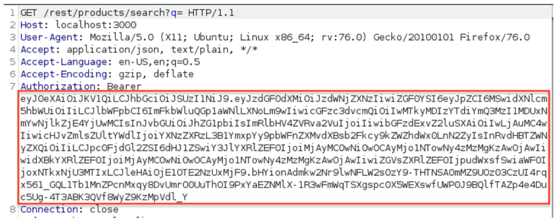
Common Use: Federated Authentication and Authorization

36

36

Often: HTTP "Authorization" Header

Remember this?



```
GET /rest/products/search?q= HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm
5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxN
mYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4w
IiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWN
yZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMC0wNi0wOCAyMjo1NTowNy4zMzMgKzAwOjAwIi
widXBkYXRlZEF0IjoiMjAyMC0wNi0wOCAyMjo1NTowNy4zMzMgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0I
joxNTkxNjU3MTIxLCJleHAiOjE1OTE2NzUxMjF9.bHYionAdmkw2Nr9lwNFLW2s0zY9-THTNSA0mMZ9U0z03CzUI4rq
x561_GQL1Tb1MnZPcnMxqy8DvUmrOOUuThOI9PxYaEZNMlX-1R3wFmWqTSXgspcOX5WEXswfUWPOJ9BQlfTAZp4e4Du
c5Ug-4T3ABK3QVf8WyZ9KzMpVdl_Y
Connection: close
```

37

37

Aside... one "obvious" reason for base64

JSON can have newlines.

HTTP headers can't.

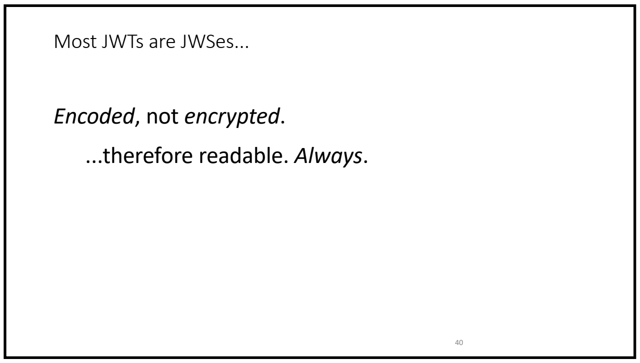
38

38

RFCs of Interest
7519: JWT (...Tokens)
7518: JWA (...Algorithms)
7515: JWS (...Signatures)
7516: JWE (...Encryption)

39

39

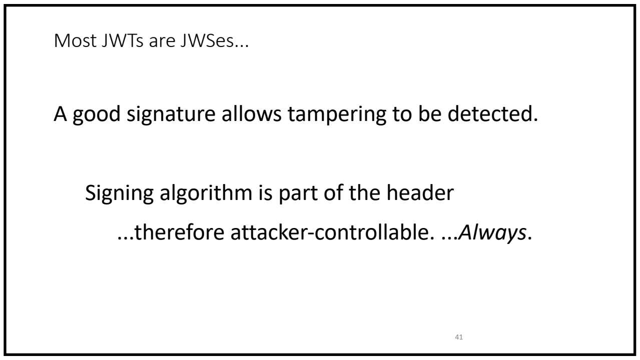


Most JWTs are JWSes...

Encoded, not *encrypted*.

...therefore readable. *Always*.

40



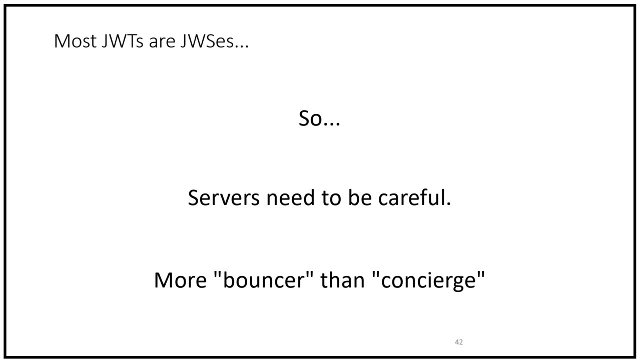
Most JWTs are JWSes...

A good signature allows tampering to be detected.

Signing algorithm is part of the header

...therefore attacker-controllable. ...*Always*.

41



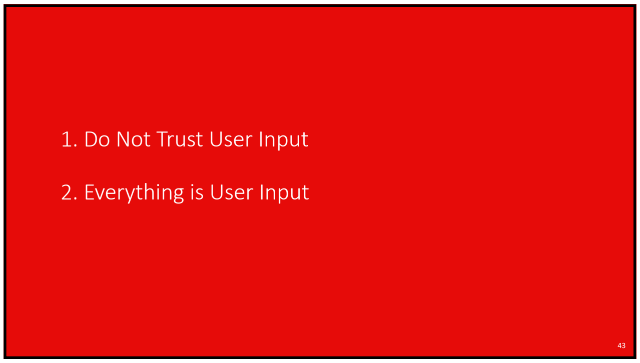
Most JWTs are JWSes...

So...

Servers need to be careful.

More "bouncer" than "concierge"

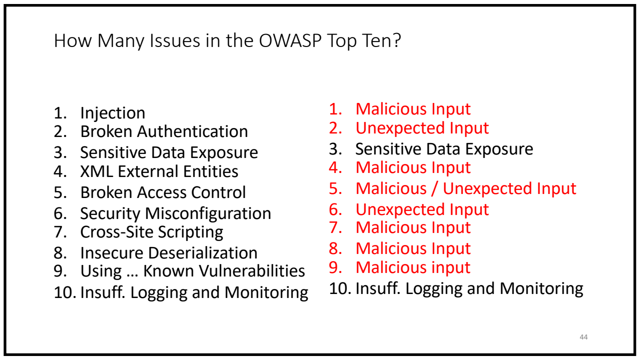
42



1. Do Not Trust User Input

2. Everything is User Input

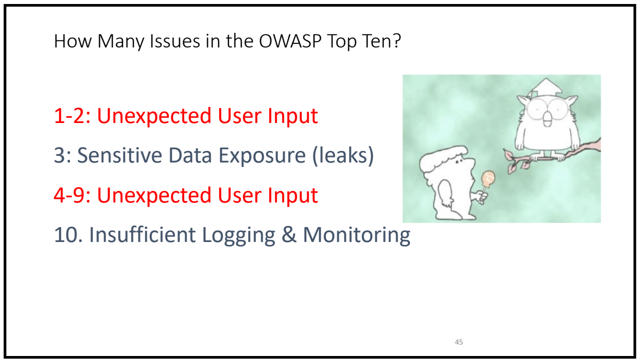
43



How Many Issues in the OWASP Top Ten?

1. Injection	1. Malicious Input
2. Broken Authentication	2. Unexpected Input
3. Sensitive Data Exposure	3. Sensitive Data Exposure
4. XML External Entities	4. Malicious Input
5. Broken Access Control	5. Malicious / Unexpected Input
6. Security Misconfiguration	6. Unexpected Input
7. Cross-Site Scripting	7. Malicious Input
8. Insecure Deserialization	8. Malicious Input
9. Using … Known Vulnerabilities	9. Malicious input
10. Insuff. Logging and Monitoring	10. Insuff. Logging and Monitoring

44



How Many Issues in the OWASP Top Ten?

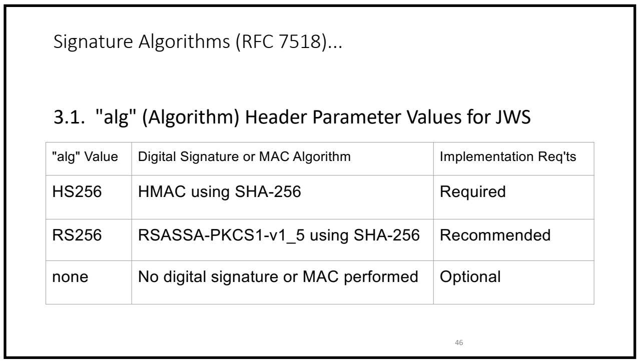
1-2: Unexpected User Input

3: Sensitive Data Exposure (leaks)

4-9: Unexpected User Input

10. Insufficient Logging & Monitoring

45



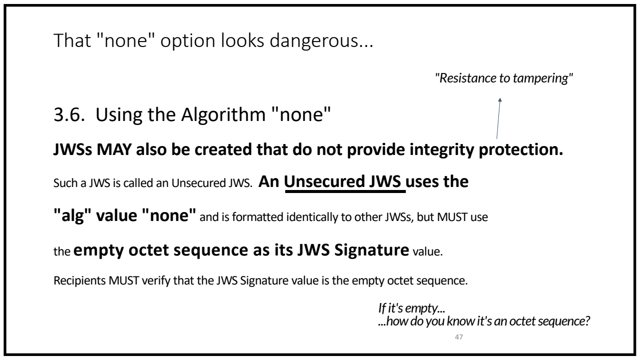
Signature Algorithms (RFC 7518)...

3.1. "alg" (Algorithm) Header Parameter Values for JWS

"alg" Value	Digital Signature or MAC Algorithm	Implementation Req'ts
HS256	HMAC using SHA-256	Required
RS256	RSASSA-PKCS1-v1_5 using SHA-256	Recommended
none	No digital signature or MAC performed	Optional

46

46



That "none" option looks dangerous...

"Resistance to tampering"

3.6. Using the Algorithm "none"

JWSs MAY also be created that do not provide integrity protection.

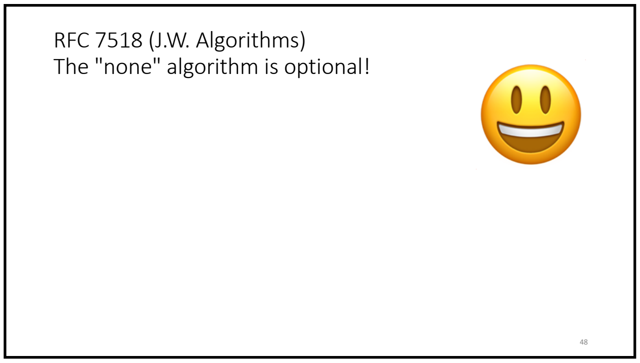
Such a JWS is called an Unsecured JWS. **An Unsecured JWS uses the "alg" value "none"** and is formatted identically to other JWSs, but MUST use the **empty octet sequence as its JWS Signature** value.

Recipients MUST verify that the JWS Signature value is the empty octet sequence.

If it's empty...
...how do you know it's an octet sequence?

47

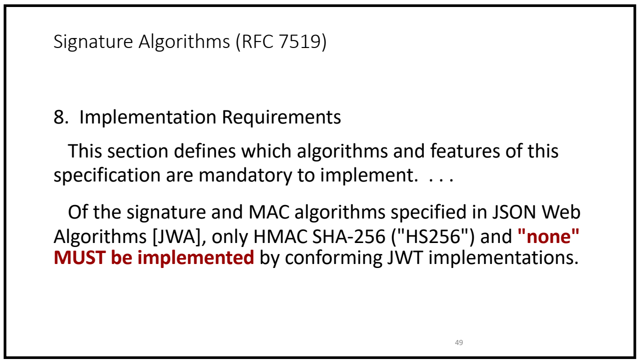
47



RFC 7518 (J.W. Algorithms)
The "none" algorithm is optional!

48

48



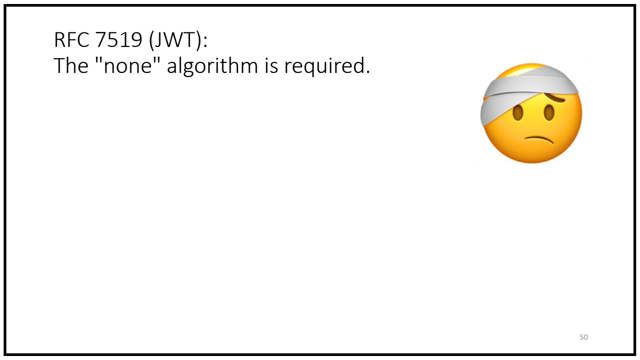
Signature Algorithms (RFC 7519)

8. Implementation Requirements

This section defines which algorithms and features of this specification are mandatory to implement. . . .

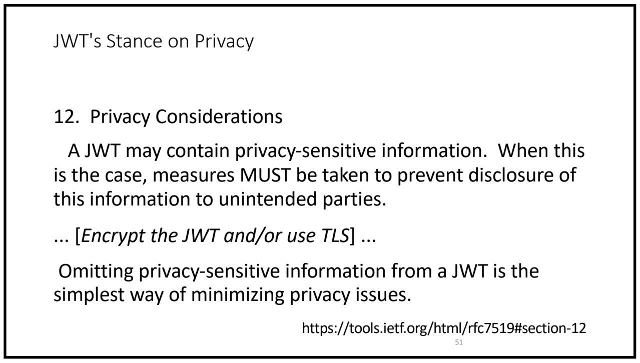
Of the signature and MAC algorithms specified in JSON Web Algorithms [JWA], only HMAC SHA-256 ("HS256") and **"none" MUST be implemented** by conforming JWT implementations.

49



RFC 7519 (JWT):
The "none" algorithm is required. 🤕

50



JWT's Stance on Privacy

12. Privacy Considerations

A JWT may contain privacy-sensitive information. When this is the case, measures MUST be taken to prevent disclosure of this information to unintended parties.

... [*Encrypt the JWT and/or use TLS*] ...

Omitting privacy-sensitive information from a JWT is the simplest way of minimizing privacy issues.

https://tools.ietf.org/html/rfc7519#section-12

51

Encrypt the JWT and/or use TLS

Edward Snowden @Snowden · Sep 21, 2016
Use Tor. Use Signal. twitter.com/Hitsmanalex/st...

This Tweet is unavailable.

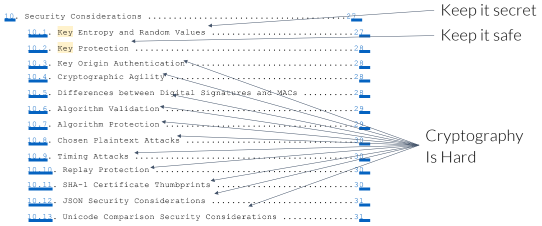
196 1.6K 2.2K

52

52

JWS's Stance on Security

(A JWS is the kind of JWT you normally see: one whose claims are not encrypted)



```
10. Security Considerations .......................................27
   10.1. Key Entropy and Random Values ...........................27
   10.2. Key Protection ..........................................28
   10.3. Key Origin Authentication ...............................28
   10.4. Cryptographic Agility ...................................28
   10.5. Differences between Digital Signatures and MACs .........28
   10.6. Algorithm Validation ....................................29
   10.7. Algorithm Protection ....................................29
   10.8. Chosen Plaintext Attacks ................................30
   10.9. Timing Attacks ..........................................30
   10.10. Replay Protection ......................................30
   10.11. SHA-1 Certificate Thumbprints ..........................30
   10.12. JSON Security Considerations ...........................31
   10.13. Unicode Comparison Security Considerations .............31
```

Keep it secret

Keep it safe

Cryptography Is Hard

53

53

...leaving us with...

No privacy protections in a JWT (*JWS*)

The "none" algorithm disables signing completely

The "none" algorithm is ... required? optional? ...both?

Attacks, then:

1. Information disclosure (just decode the payload)

2. Potential for forgery (if the "none" algorithm is supported)

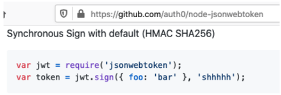
3. Cracking (guess the "secret" if 1 & 2 don't work)

54

54

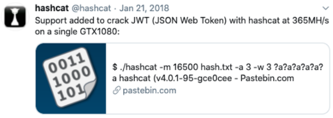
On Cracking…

- HMAC only as secure as the secret.
- JWT is self-contained.
- Sample code uses bad examples.
- Guess all day long on your own system.


https://github.com/auth0/node-jsonwebtoken

Synchronous Sign with default (HMAC SHA256)

```
var jwt = require('jsonwebtoken');
var token = jwt.sign({ foo: 'bar' }, 'shhhhh');
```


hashcat @hashcat · Jan 21, 2018

Support added to crack JWT (JSON Web Token) with hashcat at 365MH/s on a single GTX1080:

$ ./hashcat -m 16500 hash.txt -a 3 -w 3 ?a?a?a?a?a?
a hashcat (v4.0.1-95-gce0cee - Pastebin.com
pastebin.com

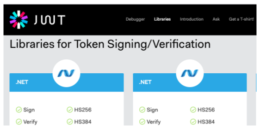
55

55

On Cracking…

- Wordlist suggestion: “secrets” from example code
  - https://github.com/BBhacKing/jwt_secrets
- Collected from all 97 projects linked at https://jwt.io/

- See also:
- https://github.com/wallarm/jwt-secrets/
- Longer list, less focused



Libraries for Token Signing/Verification

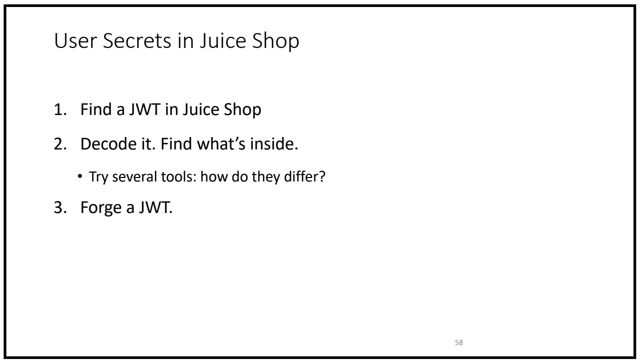
56

56

Lab #13:
JWT: Information Disclosure
JWT: Forge a JWT

57

57

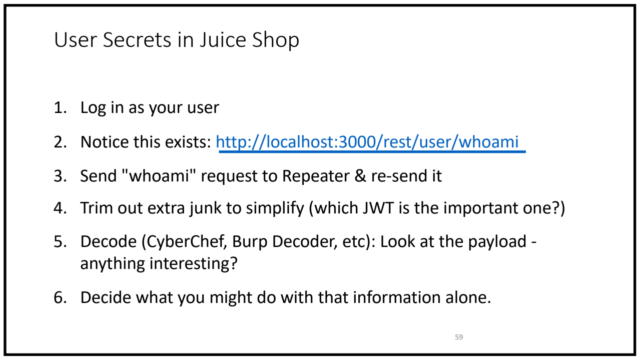


User Secrets in Juice Shop

1. Find a JWT in Juice Shop
2. Decode it. Find what’s inside.
   - Try several tools: how do they differ?
3. Forge a JWT.

58

58

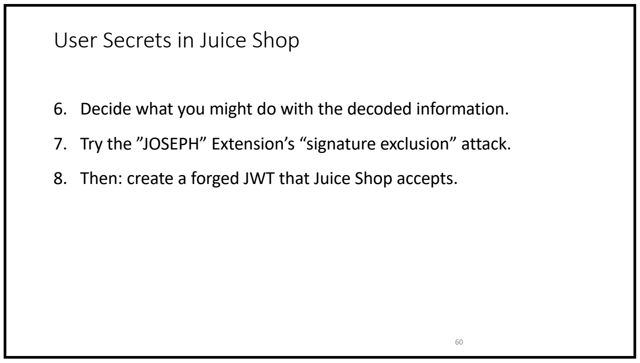


User Secrets in Juice Shop

1. Log in as your user
2. Notice this exists: http://localhost:3000/rest/user/whoami
3. Send "whoami" request to Repeater & re-send it
4. Trim out extra junk to simplify (which JWT is the important one?)
5. Decode (CyberChef, Burp Decoder, etc): Look at the payload - anything interesting?
6. Decide what you might do with that information alone.

59

59

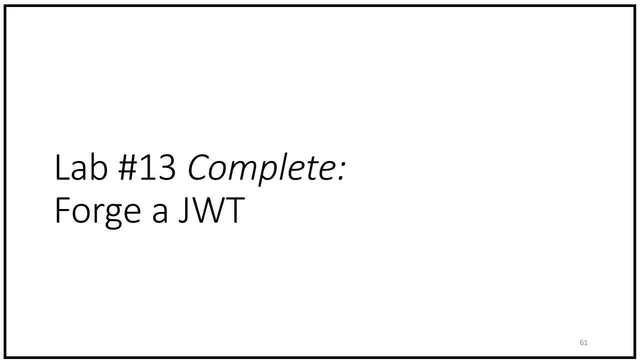


User Secrets in Juice Shop

6. Decide what you might do with the decoded information.
7. Try the ”JOSEPH” Extension’s “signature exclusion” attack.
8. Then: create a forged JWT that Juice Shop accepts.

60

60



Lab #13 *Complete:*
Forge a JWT

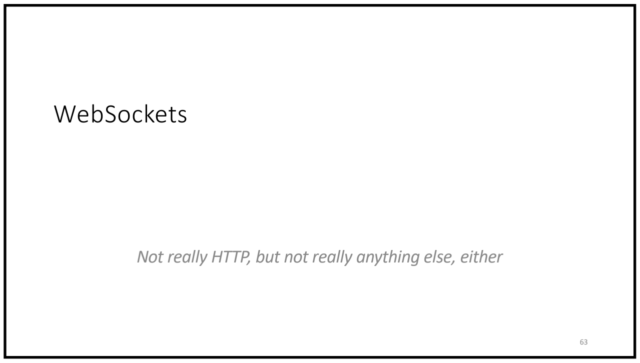
61

61

What's Your Takeaway from the Lab?

62

62

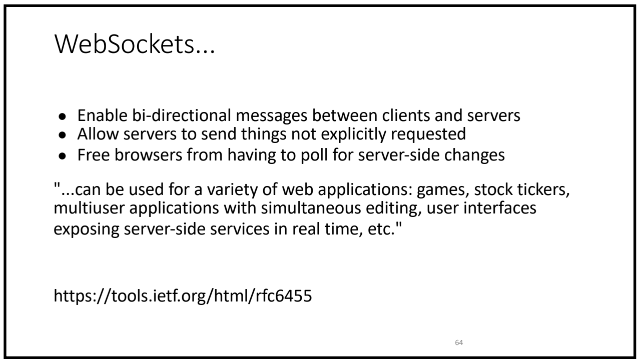


WebSockets

Not really HTTP, but not really anything else, either

63

63



WebSockets...

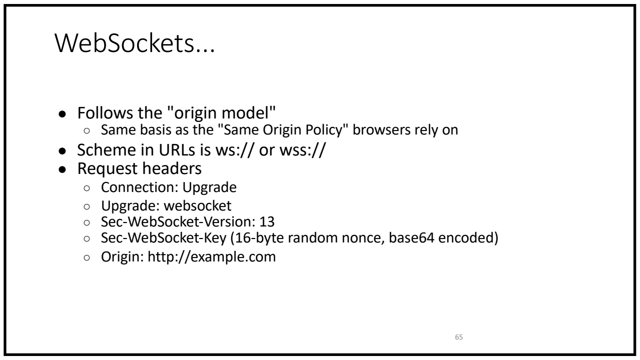
- Enable bi-directional messages between clients and servers
- Allow servers to send things not explicitly requested
- Free browsers from having to poll for server-side changes

"...can be used for a variety of web applications: games, stock tickers, multiuser applications with simultaneous editing, user interfaces exposing server-side services in real time, etc."

https://tools.ietf.org/html/rfc6455

64

64

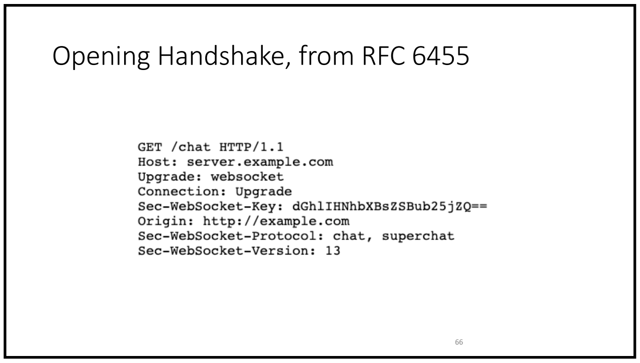


WebSockets...

- Follows the "origin model"
  - Same basis as the "Same Origin Policy" browsers rely on
- Scheme in URLs is ws:// or wss://
- Request headers
  - Connection: Upgrade
  - Upgrade: websocket
  - Sec-WebSocket-Version: 13
  - Sec-WebSocket-Key (16-byte random nonce, base64 encoded)
  - Origin: http://example.com

65

65



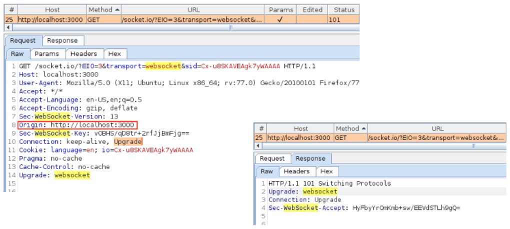
Opening Handshake, from RFC 6455

```
GET /chat HTTP/1.1
Host: server.example.com
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: dGhlIHNhbXBsZSBub25jZQ==
Origin: http://example.com
Sec-WebSocket-Protocol: chat, superchat
Sec-WebSocket-Version: 13
```

66

66

Opening Handshake, from Juice Shop



#	Host	Method ▲	URL	Params	Edited	Status
25	http://localhost:3000	GET	/socket.io/?EIO=3&transport=websocket&...	✓		101

```
GET /socket.io/?EIO=3&transport=websocket&sid=Cx-u8SKAVEAgk7yWAAAA HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:77.0) Gecko/20100101 Firefox/77
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Sec-WebSocket-Version: 13
Origin: http://localhost:3000
Sec-WebSocket-Key: vOBHS/qD8tr+2rfJjBmFjg==
Connection: keep-alive, Upgrade
Cookie: language=en; io=Cx-u8SKAVEAgk7yWAAAA
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket
```

#	Host	Method ▲	URL
25	http://localhost:3000	GET	/socket.io/?EIO=3&transport=websocket&...

```
HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: HyFbyYrOmKmb+sw/EEVdSTLh9gQ=
```

WebSocket Security

HTTP Response Header "Sec-WebSocket-Accept" is...

sec-websocket-key from the request

with a constant RFC-specified GUID appended

SHA-1 hash

Base64 Encode

```
base64(sha1(vOBHS/qD8tr+2rfJjBmFjg==258EAFA5-E914-47DA-95CA-
C5AB0DC85B11))
```

```
Yields this: HyFbyYrOmKmb+sw/EEVdSTLh9gQ=
```

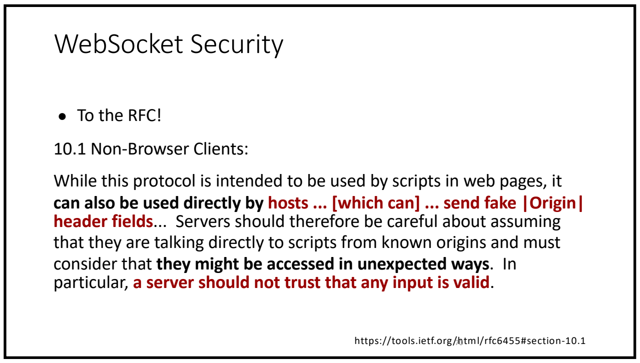
WebSocket Security

Server knows it's a legit client because of the Origin request header.

...unless it's not a browser

Client knows it's talking to legit server because the client provided the randomness that's part of the web-socket-accept header in the response...

Wait.



WebSocket Security

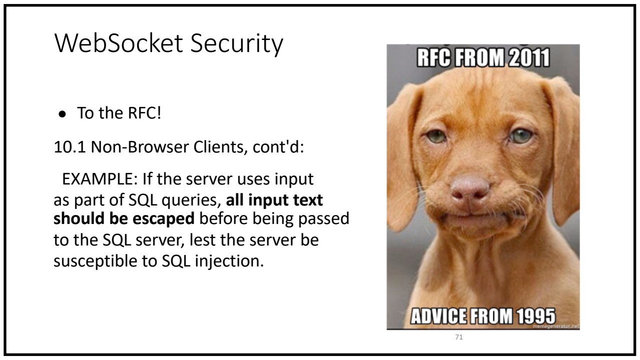
- To the RFC!

10.1 Non-Browser Clients:

While this protocol is intended to be used by scripts in web pages, it **can also be used directly by hosts ... [which can] ... send fake |Origin| header fields**... Servers should therefore be careful about assuming that they are talking directly to scripts from known origins and must consider that **they might be accessed in unexpected ways**. In particular, **a server should not trust that any input is valid**.

https://tools.ietf.org/html/rfc6455#section-10.1

70



WebSocket Security

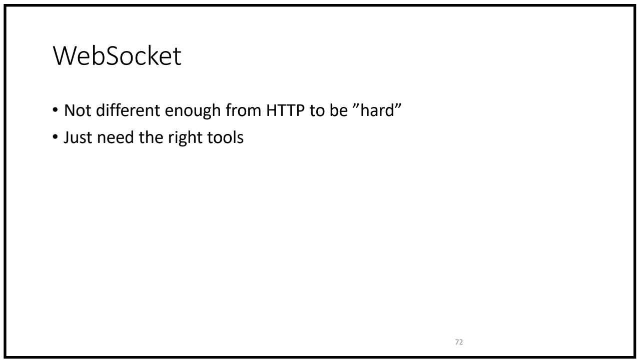
- To the RFC!

10.1 Non-Browser Clients, cont'd:

EXAMPLE: If the server uses input as part of SQL queries, **all input text should be escaped** before being passed to the SQL server, lest the server be susceptible to SQL injection.

71

71



WebSocket

- Not different enough from HTTP to be ”hard”
- Just need the right tools

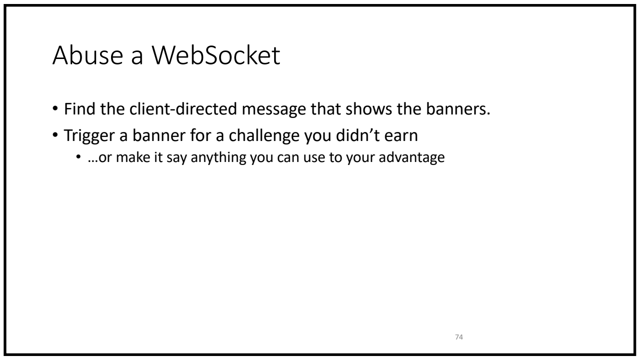
72

72

Lab #14:
Abuse a Web Socket

73

73



Abuse a WebSocket

- Find the client-directed message that shows the banners.
- Trigger a banner for a challenge you didn’t earn
    - …or make it say anything you can use to your advantage

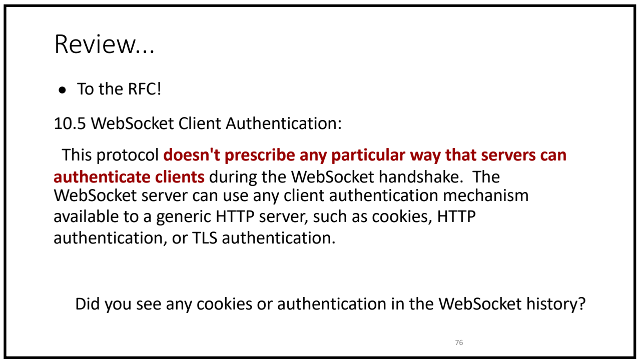
74

74

Lab #14 *Complete:*
Abuse a Web Socket

75

75



Review...

- To the RFC!

10.5 WebSocket Client Authentication:

This protocol **doesn't prescribe any particular way that servers can authenticate clients** during the WebSocket handshake. The WebSocket server can use any client authentication mechanism available to a generic HTTP server, such as cookies, HTTP authentication, or TLS authentication.

Did you see any cookies or authentication in the WebSocket history?

76

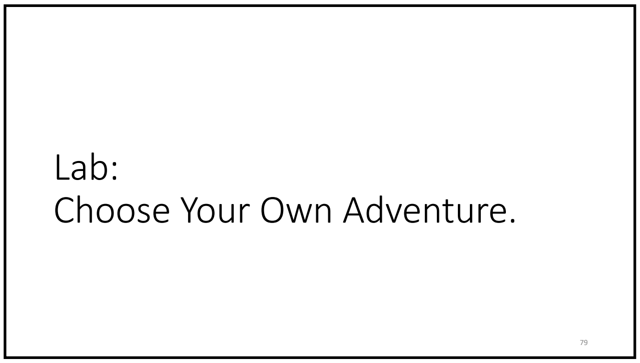
What's Your Takeaway from the Lab?

77

Webapp Pentesting is *Advanced "Paying Attention"*

...once you know what to look for.

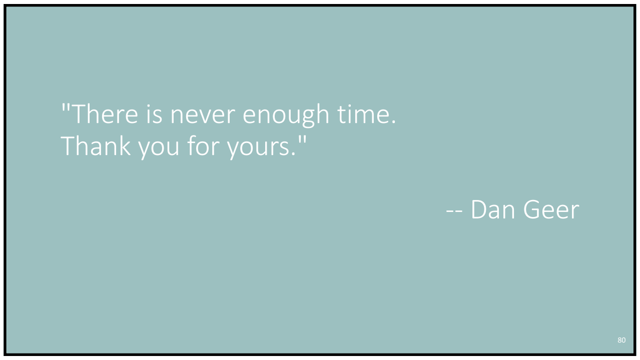
78



Lab:
Choose Your Own Adventure.

79

79



"There is never enough time.
Thank you for yours."

-- Dan Geer

80

80