





BISHOPFOX

Andrew Wilson

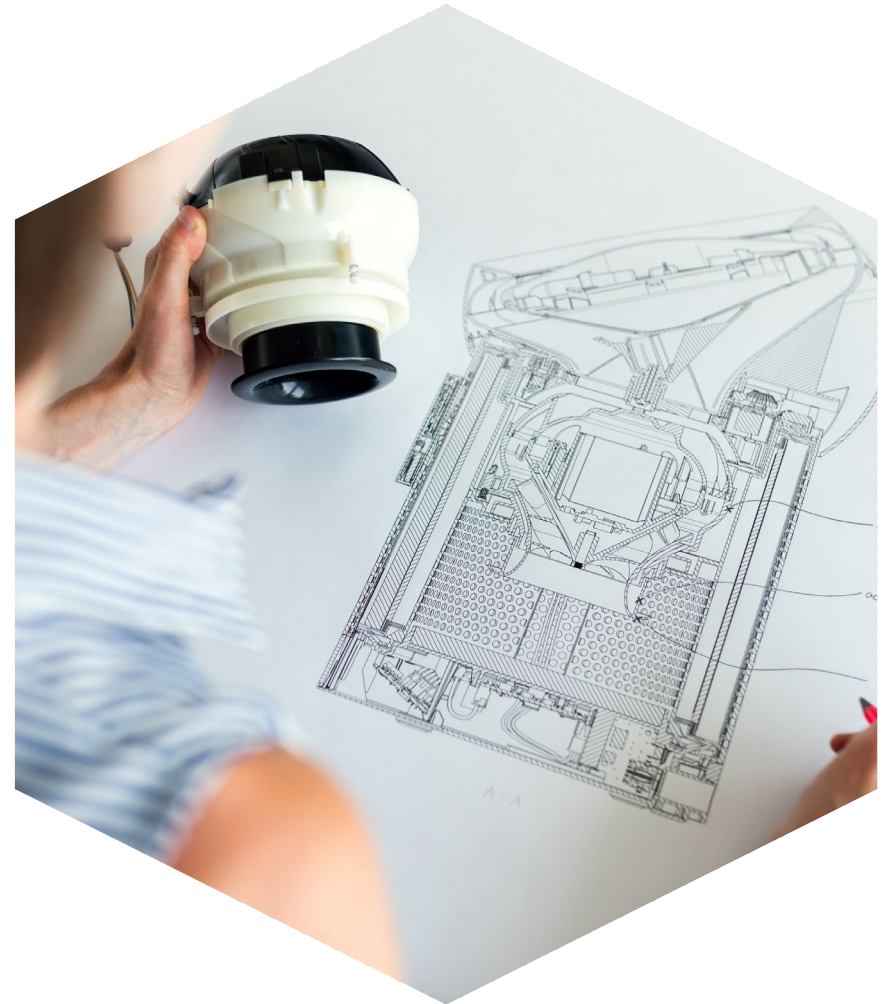
@ K U Z U S H I

- Vice President of Consulting at Bishop Fox
- Sen Security Project (sensecurity.io)
- Co-founder of CactusCon
- Software Engineer for 10 years
- Application Security Tester for 10 years

Security testing is,
first and foremost,
a visibility problem
-@tqbf

In Practical Terms:

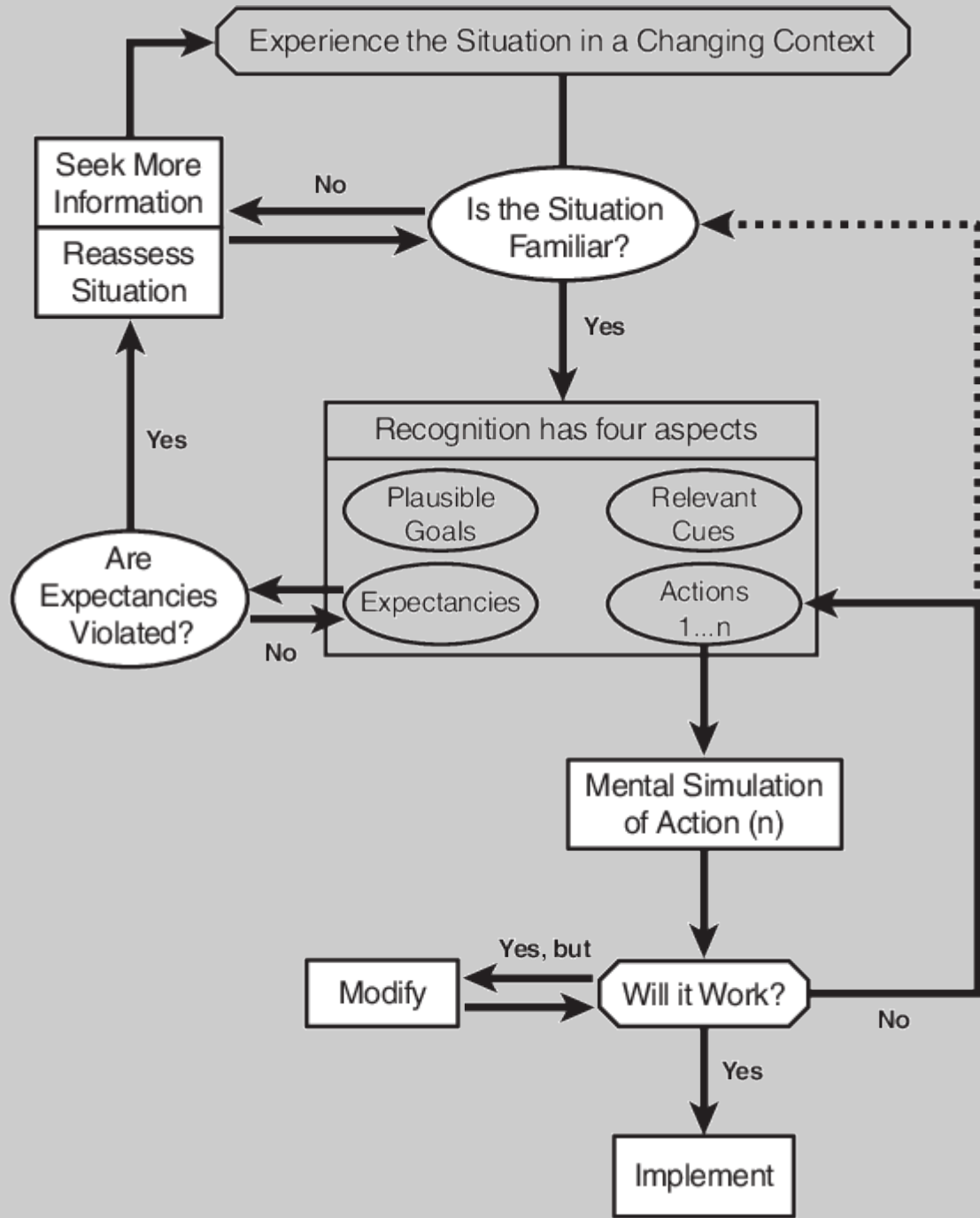
- Knowledge of systems leads to identifying weaknesses in them.
- Knowledge of a specific system leads to building reliable exploits



A man with short dark hair, wearing a dark t-shirt, is looking out of a window at night. The background is a blurred cityscape with lights. The text is overlaid on the left side of the image.

Limitations

- No guarantee of a homecourt advantage
- Not always a full picture
- No set standards
(except for the standards)



Recognition Primed Decision Making

NATURALISTIC DECISIONS

1. Pattern matching as a means to solve time-gapped problems with incomplete information
2. Recognition is near instantly, relying heavily on understanding components of problems
3. Gary Klein, Sources of Power

Inductive Method

"**Wherever** he steps, **whatever** he touches, **whatever** he leaves, even unconsciously, will serve as a silent witness against him. – Edmond Locard



Deductive Methods

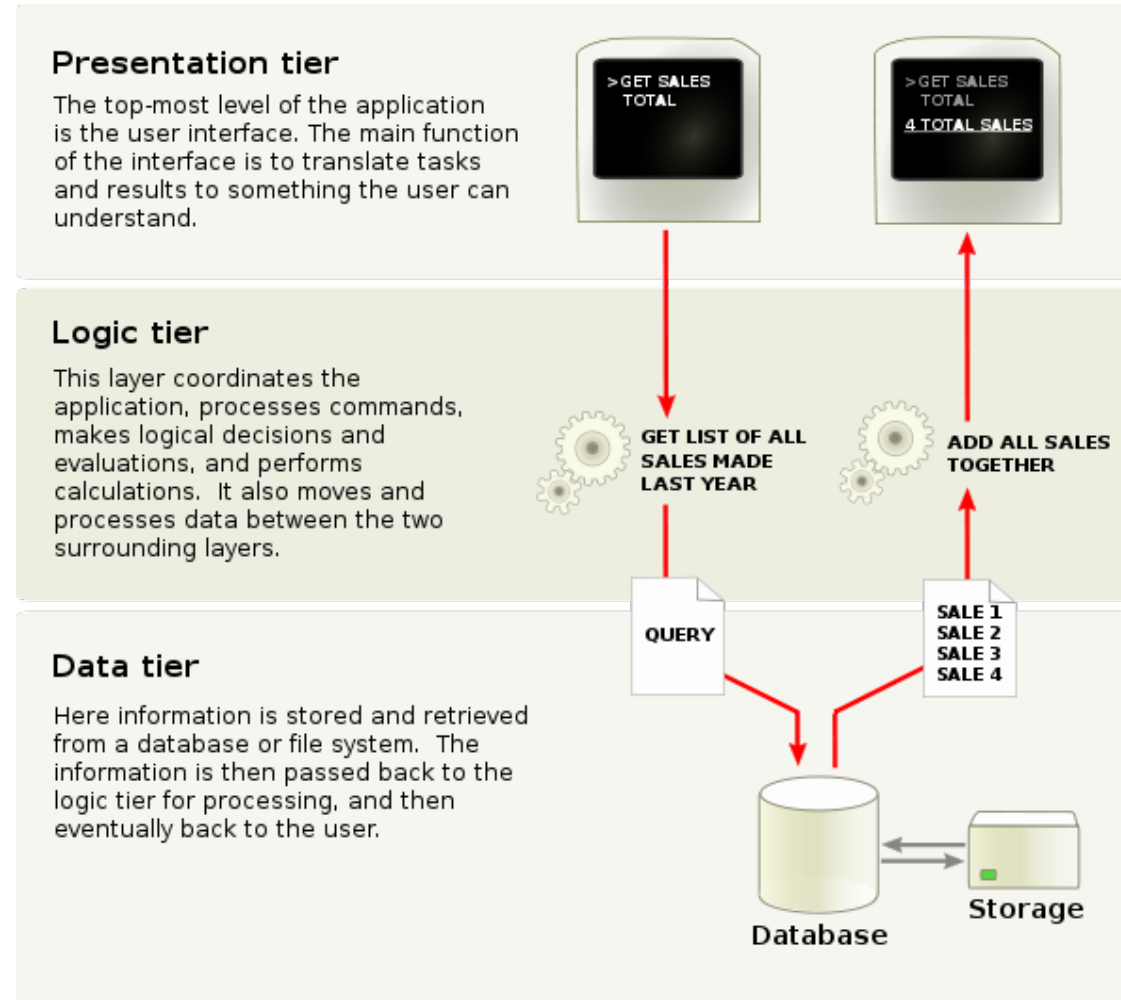
All men or mortal
Socrates is a man
Therefore, Socrates is mortal

je pense, donc je suis

Basic Application Design

Fundamental Composition

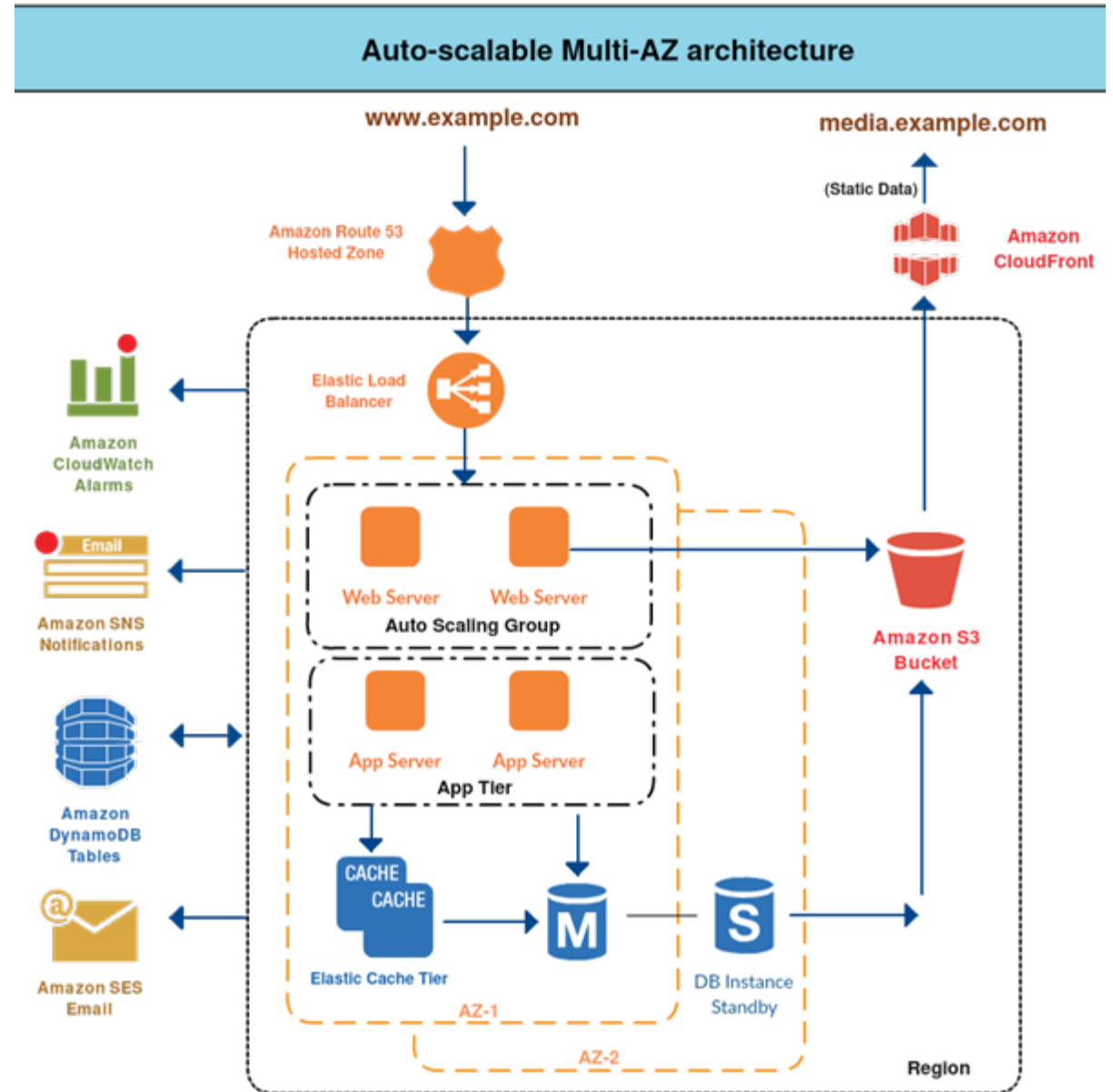
1. Presentation tier displays data, gets new data
2. Logic tier parses rules, handles data routing
3. Data tier stores all the data



(Semi) Modern Deployment

Application of Basics

1. Load balancers to balance load
2. Web Servers to auto scale on demand
3. App tier to scale to support load
4. Cache to reduce database calls
5. Static content served from dedicated space
6. External monitoring of internal activities



WIKIPEDIA

The Free Encyclopedia

English

6 183 000+ articles

Español

1 637 000+ artículos

日本語

1 235 000+ 記事

Deutsch

2 495 000+ Artikel

Русский

1 672 000+ статей

Français

2 262 000+ articles

Italiano

1 645 000+ voci

中文

1 155 000+ 條目

Português

1 045 000+ artigos

Polski

1 435 000+ haseł



CASE STUDY: Wikipedia

HOW DO THY SERVE

```
HTTP/1.1 304 Not Modified
Date: Tue, 10 Nov 2020 05:53:58 GMT
Cache-Control: s-maxage=86400, must-revalidate, max-age=3600
Server: ATS/8.0.8
ETag: W/"10d12-5b31e183d96b7"
Last-Modified: Mon, 02 Nov 2020 11:32:00 GMT
Content-Type: text/html
Vary: Accept-Encoding
Age: 84605
X-Cache: cp5009 hit, cp5007 hit/327888
X-Cache-Status: hit-front
Server-Timing: cache;desc="hit-front"
Strict-Transport-Security: max-age=106384710; includeSubDomains; preload
Report-To: { "group": "wm_nel", "max_age": 86400, "endpoints": [{ "url": "https://intake-logging.wikimedia.org/v1/events?stream=w3c.reportingapi.network_error&schema_uri=/w3c/reportingapi/network_error/1.0.0" }] }
NEL: { "report_to": "wm_nel", "max_age": 86400, "failure_fraction": 0.05, "success_fraction": 0.0 }
Set-Cookie: WMF-Last-Access=11-Nov-2020;Path=/;HttpOnly;secure;Expires=Sun, 13 Dec 2020 00:00:00 GMT
X-Client-IP: 212.102.50.198
Connection: close
```

1. Server = Apache Traffic Server
2. X-Cache = Served from Cache
3. Report-To = logging host via NEL
4. Sets a home cookie (WMF Last Access)
5. Identifies my IP via header

What did we learn?

1. Confirmed that the pages are served via Cache
2. Identified technology of cache
3. Figured out how they are likely tracking us

What don't we know?

1. How do we get to real servers?
2. What are other types of servers are likely in play?
3. Does geography affect where I land?

WIKIPEDIA

The Free Encyclopedia

English

6 183 000+ articles

Español

1 637 000+ artículos

日本語

1 235 000+ 記事

Русский

1 672 000+ статей

Italiano

1 645 000+ voci

Português

1 045 000+ artigos

Deutsch

2 495 000+ Artikel

Français

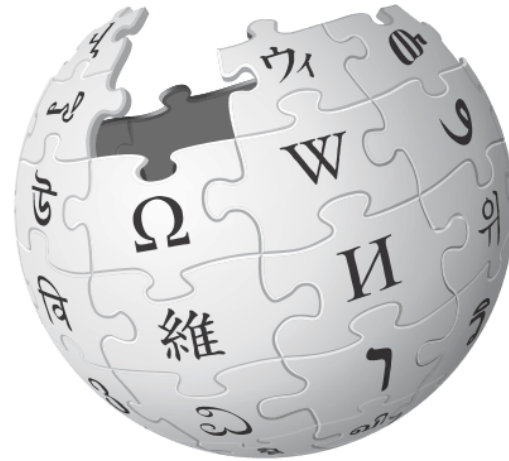
2 262 000+ articles

中文

1 155 000+ 條目

Polski

1 435 000+ haseł



Welcome to Wikipedia,

the [free encyclopedia](#) that [anyone can edit](#).
6,189,874 articles in English

- [The arts](#)
- [History](#)
- [Society](#)
- [Biography](#)
- [Mathematics](#)
- [Technology](#)
- [Geography](#)
- [Science](#)
- [All portals](#)

From today's featured article



First X-ray laser

Project Excalibur was an American [Cold War](#)–era research program to develop nuclear-device-powered, space-based [X-ray lasers](#) as a [ballistic missile defense](#). X-ray lasers were conceived in the 1970s by [George Chapline Jr.](#) (*pictured with George Maenchen*) and further developed by [Peter L. Hagelstein](#), both working at [Lawrence Livermore National Laboratory](#) under [Edward Teller](#). After a promising test, Teller discussed the proposal in 1981 with US president [Ronald Reagan](#), who in 1983 incorporated it in his [Strategic Defense Initiative](#). Further [underground nuclear tests](#) suggested progress was being made. Reagan refused to abandon the technology at the 1986 [Reykjavík Summit](#) arms-control talks, even after a critical test demonstrated it was not working as expected. Researchers at Livermore and [Los Alamos](#) began to raise concerns about test results, and the infighting became public. In 1988 the program budget was cut dramatically, after additional problems were revealed. ([Full article...](#))

Recently featured: [Edward Thomas Daniell](#) · [St. Croix macaw](#) · [Fabian Ware](#)
[Archive](#) · [By email](#) · [More featured articles](#)

Did you know ...

- ... that on this day, Nepali people [worship dogs](#) (*example pictured*) to please [Yama](#)?



In the news

COVID-19 pandemic: [Disease](#) · [Virus](#) · [By location](#) · [Impact](#) · [Portal](#)

- [Manuel Merino](#) becomes [President of Peru](#) after [Martín Vizcarra](#) (*pictured*) is impeached and removed from office.
- Armenia and Azerbaijan sign a Russian-brokered [ceasefire agreement](#) to end the [Nagorno-Karabakh war](#).
- In [cricket](#), the [Indian Premier League](#) concludes with the [Mumbai Indians](#) defeating the [Delhi Capitals](#) in [the final](#).
- In [stock car racing](#), [Chase Elliott](#) wins [the NASCAR Cup Series](#).



Martín Vizcarra

Recent deaths: [Peter Sutcliffe](#) · [Jerry Rawlings](#) · [Abdulkadir Balarabe Musa](#) · [Amadou Toumani Touré](#) · [Sven Wollter](#) · [Saeb Erekat](#)

[Other recent events](#) · [Nominate an article](#)

On this day

November 14: World Diabetes Day

- 1680 – German astronomer



CASE STUDY: Wikipedia

HOW DO THY SERVE (dynamic)

```
HTTP/1.1 301 Moved Permanently
Date: Mon, 09 Nov 2020 02:22:23 GMT
Server: mw1413.eqiad.wmnet
X-Content-Type-Options: nosniff
P3p: CP="See https://en.wikipedia.org/wiki/Special:CentralAutoLogin/P3P for more info."
Vary: Accept-Encoding,X-Forwarded-Proto,Cookie,Authorization
Cache-Control: s-maxage=1200, must-revalidate, max-age=0
X-Request-Id: 55a6e13c-2b91-4600-a1f7-20a8d358ffe6
Last-Modified: Mon, 09 Nov 2020 02:22:23 GMT
Location: https://en.wikipedia.org/wiki/Main_Page
```

1. Server = mw1413.eqiad.wmnet
2. Not served from cache
3. "X-Request-ID" == Logging ?

I requested:

https://en.wikipedia.org/wiki/Main_Page

But viewsource shows:


Retrieved from "<a dir="ltr"
href="https://en.wikipedia.org/w/index.php?title=Main_Page&oldid=987965326">

?



User:ST47 - Wikipedia

https://en.wikipedia.org/w/index.php?title=User:ST47



WIKIPEDIA
The Free Encyclopedia

[Main page](#)
[Contents](#)
[Current events](#)
[Random article](#)
[About Wikipedia](#)

User page [Talk](#)


User:ST47

From Wikipedia, the free encyclopedia

Hello! I'm an admin, checkuser, and overseight, if you have a que private information, or [WP:RAA](#) for other administrative requests.

Tools

← → ↻ 🔒 <https://en.wikipedia.org/wiki/User:ST47>



WIKIPEDIA
The Free Encyclopedia

[Main page](#)
[Contents](#)
[Current events](#)
[Random article](#)
[About Wikipedia](#)
[Contact us](#)
[Donate](#)

User page [Talk](#)

User:ST47

From Wikipedia, the free encyclopedia

Hello! I'm an admin, checkuser, and overseight private information, or [WP:RAA](#) for other administrative requests.

Tools

- [Search page history for a given string or](#)
- [Search for usernames matching a given](#)

Copyrighted Material

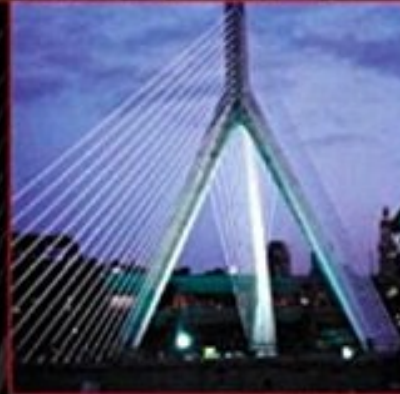
The Addison-Wesley Signature Series

PATTERNS OF ENTERPRISE APPLICATION ARCHITECTURE

A MARTIN FOWLER SIGNATURE
BOOK
Martin

MARTIN FOWLER

WITH CONTRIBUTIONS BY
DAVID RICE,
MATTHEW FOEMMEL,
EDWARD HEATT,
ROBERT MEE, AND
RANDY STAFFORD

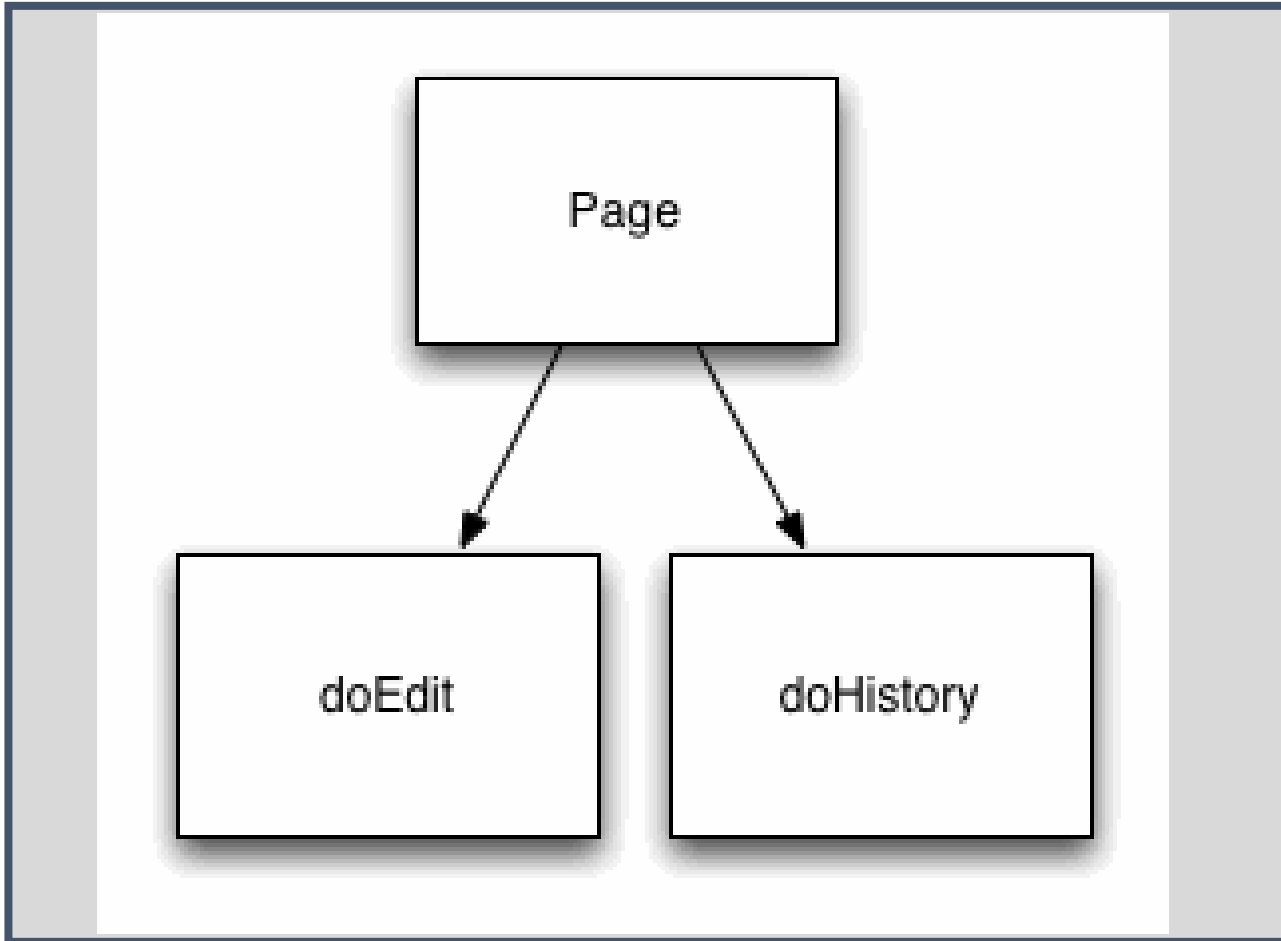


Copyrighted Material

<https://martinfowler.com/eaCatalog/>

CASE STUDY: Wikipedia

How are pages served?

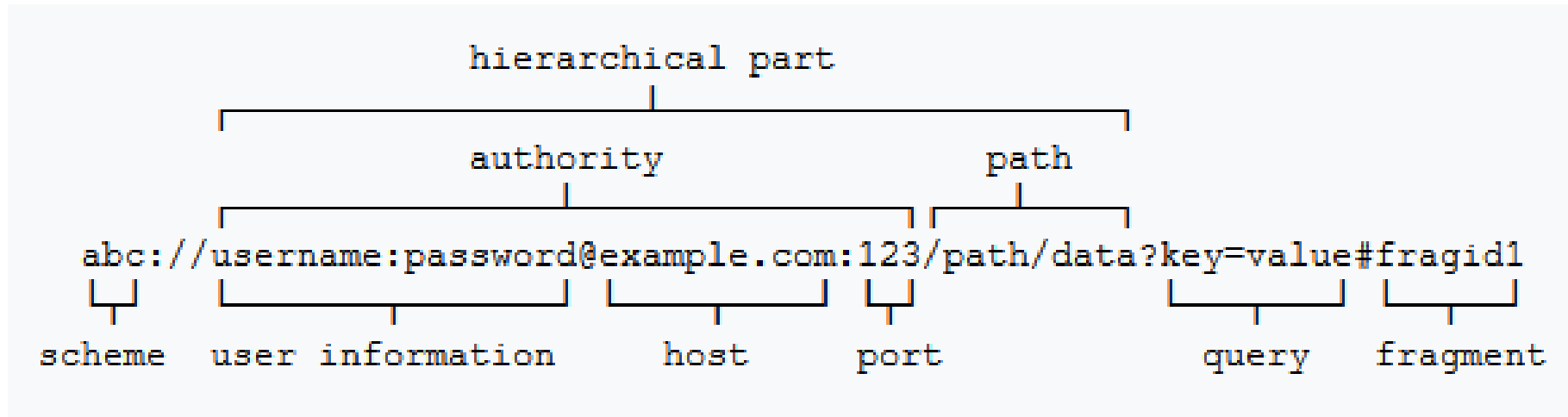


1. Front controller is typically following a pattern of: `page.php?action=<x>¶m=y`

2. It also means that the 2nd route is likely a regex or aliasing map to this call

3. Given how frequently this shows up, it is likely primary means content is served

Standards (someone has to have them)



Now here is where things get *spicy*

- ? title=Main_Page&oldid=986033447
- ? title=Main_Page&printable=yes
- ? title=Special:CiteThisPage&page=Main_Page&id=986033447&wpFormIdentifier=titleform
- ? title=Special:CreateAccount&returnto=Main+Page
- ? title=Special:CreateAccount&returnto=User%3AST47
- ? title=Special:CreateAccount&returnto=User%3AST47%2F
- ? title=Special:CreateAccount&returnto=User%3AST47%2Fmarkblocked.js
- ? title=Special:CreateAccount&returnto=User%3AST47%2Fmarkblocked.js&returntoquery=action%3Dedit
- ? title=Special:CreateAccount&returnto=Wikipedia%3ASockpuppet+investigations
- ? title=Special:CreateAccount&returnto=Wikipedia%3ASockpuppet+investigations%2FSPI%2FClerks
- ? title=Special:DownloadAsPdf&page=Main_Page&action=show-download-screen
- ? title=Special:DownloadAsPdf&page=User%3AST47%2Fmarkblocked.js&action=show-download-screen
- ? title=Special:DownloadAsPdf&page=User%3AST47&action=show-download-screen
- ? title=Special:DownloadAsPdf&page=Wikipedia%3ASockpuppet_investigations%2FSPI%2FClerks&acti ...
- ? title=Special:DownloadAsPdf&page=Wikipedia%3ASockpuppet_investigations&action=show-download-s
- ? title=Special:Log/delete&page=User:ST47/
- ? title=Special:Search&search={searchTerms
- ? title=Special:UserLogin&returnto=Main+Page
- ? title=Special:UserLogin&returnto=User%3AST47
- ? title=Special:UserLogin&returnto=User%3AST47%2F

Hello! I'm an admin, checkuser, and oversighter, if you have a question or a case, please visit [WP:SPI](#) for checkuser requests, email [oversight](#)

Tools

- [Search page history for a given string or regex](#)
- [Search for usernames matching a given string or regex](#)
- [Beta WHOIS tool for fetching extra information about an IP address](#)
- [User:ST47/markblocked.js](#) - Fork of [MediaWiki:Gadget-markblocked.js](#)
- [User:ST47/culoghelper.js](#) - Fork of [User:Amalthea/culoghelper.js](#)
- [User:ST47/cu-log-links.js](#) - Adds links to whois, contribs, profile, and CU log

Links

- [/rangeblocks expiring soon](#)
- [/global rangeblocks expiring soon](#)
- [/high block density](#)
- [/overspecific v6 blocks](#)
- [/cogent](#)
- [/softblocked proxies](#)
- [/indef-blocked ips](#)

Served As: HTML

WIKIPEDIA

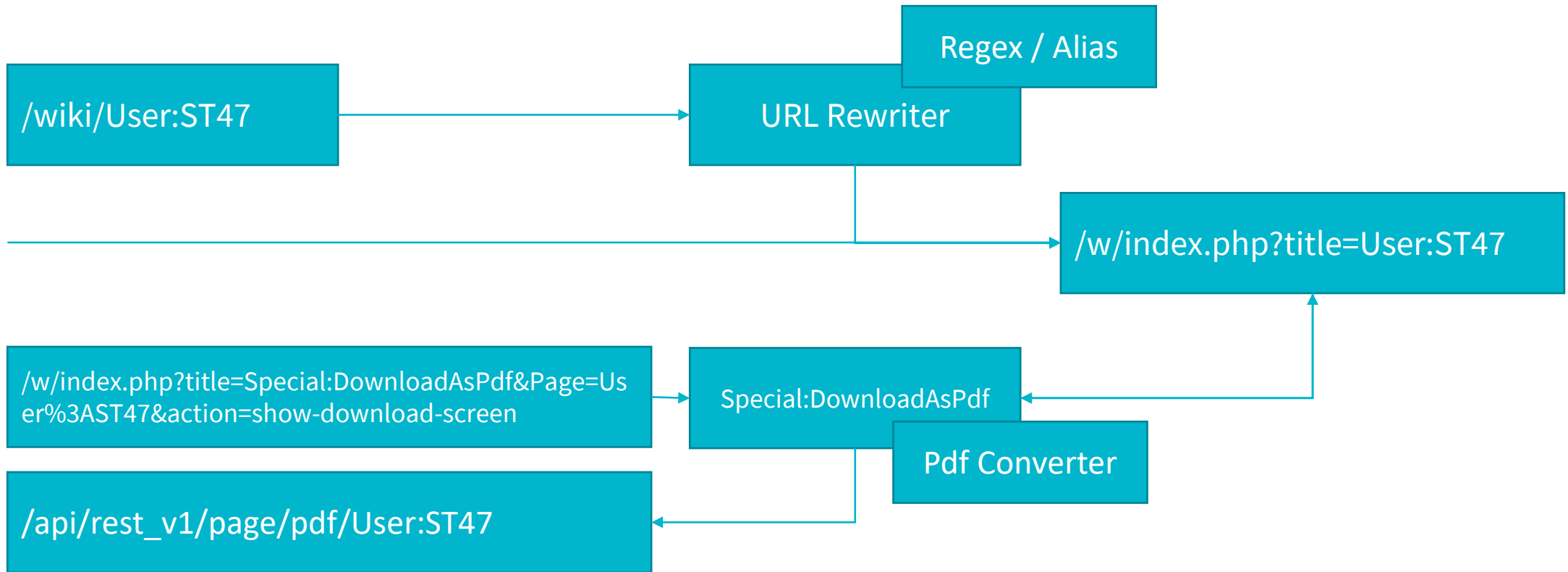
User:ST47

Hello! I'm an admin, checkuser, and oversighter, if you have a question or a case, please visit my [talk page](#) and leave a message. If you require assistance with checkuser requests, email [oversight](#) to request [suppression](#) of email. For [WP:RAA](#) for other administrative requests.

Tools

- [Search page history for a given string or regex \(https://tools.wmflabs.org/pagehistory/\)](#)
- [Search for usernames matching a given string or regex \(https://tools.wmflabs.org/username/\)](#)
- [Beta WHOIS tool for fetching extra information about an IP address \(https://tools.wmflabs.org/whois-referral/gateway.py\)](#)
- [User:ST47/markblocked.js](#) - Fork of [MediaWiki:Gadget-markblocked.js](#) - tends to manifest on [CAT:UNB](#)
- [User:ST47/culoghelper.js](#) - Fork of [User:Amalthea/culoghelper.js](#)
- [User:ST47/cu-log-links.js](#) - Adds links to whois, contribs, profile, and CU log

Served As: PDF



What did we learn?

1. Identified Language of Website
2. Identified Request Patterns
3. Names of specific functions (this mechanism for 1 page, is same for n-pages just like it)
4. Identified a super user account

What don't we know?

1. What are the interesting other pages?
2. What other actions does each page support?
3. How do the edge nodes know how to match requesting patterns?
4. What sort of encoding protections do they have based on two types of patterns?
5. Who is this *punk* who blocked me?

CASE STUDY: Wikipedia

Breaking Cache

```
GET
/w/load.php?lang=en&modules=ext.TemplateWizard%7Cext.TwoColConflict.JSCheck%7Cjquery%2Coojs-ui-core%2Coojs-ui-widgets%7Cjquery.ui%7Cmediawiki.action.edit%7Cmediawiki.action.edit.editWarning%7Cmediawiki.language.specialCharacters%7Cmediawiki.template%7Cmediawiki.widgets.DateInputWidget%2CUserInputWidget%7Cmediawiki.widgets.DateInputWidget.styles%7Coojs-ui.styles.icons-editing-citation%2Cicons-editing-list%2Cicons-media%7Cwikibase.client.action.edit.collapsibleFooter&skin=vector&version=1645t
```

```
HTTP/1.1 200 OK
Date: Thu, 12 Nov 2020 05:11:43 GMT
Server: mw1364.eqiad.wmnet
X-Content-Type-Options: nosniff
Cache-Control: public, max-age=2592000, s-maxage=2592000
Expires: Sat, 12 Dec 2020 05:11:43 GMT
Vary: Accept-Encoding
X-Request-Id: 13daaae6-d017-468d-98db-df86860f3627
Etag: W/"1645t"
Content-Type: text/javascript; charset=utf-8
X-Cache: cp4032 miss, cp4027 miss
X-Cache-Status: miss
Server-Timing: cache;desc="miss"
Strict-Transport-Security: max-age=106384710; includeSubDomains; preload
Report-To: { "group": "wm_nel", "max_age": 86400, "endpoints": [{ "url": "https://intake-logging.wikimedia.org/v1/events?stream=w3c.reportingapi.network_error&schema_uri=/w3c/reportingapi/network_error/1.0.0" }] }
NEL: { "report_to": "wm_nel", "max_age": 86400, "failure_fraction": 0.05, "success_fraction": 0.0}
X-Client-IP: 72.211.19.239
```

Welcome to Wikipedia,

the [free encyclopedia](#) that [anyone can edit](#).

6,189,874 articles in English

- [The arts](#)
- [History](#)
- [Society](#)
- [Biography](#)
- [Mathematics](#)
- [Technology](#)
- [Geography](#)
- [Science](#)
- [All portals](#)

From today's featured article



First X-ray laser

Project Excalibur was an American [Cold War](#)–era research program to develop nuclear-device-powered, space-based [X-ray lasers](#) as a [ballistic missile defense](#). X-ray lasers were conceived in the 1970s by [George Chapline Jr.](#) (*pictured with George Maenchen*) and further developed by [Peter L. Hagelstein](#), both working at [Lawrence Livermore National Laboratory](#) under [Edward Teller](#). After a promising test, Teller discussed the proposal in 1981 with US president [Ronald Reagan](#), who in 1983 incorporated it in his [Strategic Defense Initiative](#). Further

[underground nuclear tests](#) suggested progress was being made. Reagan refused to abandon the technology at the 1986 [Reykjavík Summit](#) arms-control talks, even after a critical test demonstrated it was not working as expected. Researchers at Livermore and [Los Alamos](#) began to raise concerns about test results, and the infighting became public. In 1988 the program budget was cut dramatically, after additional problems were revealed. ([Full article...](#))

Recently featured: [Edward Thomas Daniell](#) · [St. Croix macaw](#) · [Fabian Ware](#)
[Archive](#) · [By email](#) · [More featured articles](#)

Did you know ...

- ... that on this day, Nepali people [worship dogs](#) (*example pictured*) to please [Yama](#)?



In the news

COVID-19 pandemic: [Disease](#) · [Virus](#) · [By location](#) · [Impact](#) · [Portal](#)

- [Manuel Merino](#) becomes [President of Peru](#) after [Martín Vizcarra](#) (*pictured*) is impeached and removed from office.
- Armenia and Azerbaijan sign a Russian-brokered [ceasefire agreement](#) to end the [Nagorno-Karabakh war](#).
- In [cricket](#), the [Indian Premier League](#) concludes with the [Mumbai Indians](#) defeating the [Delhi Capitals](#) in [the final](#).
- In [stock car racing](#), [Chase Elliott](#) wins [the NASCAR Cup Series](#).



Martín Vizcarra

Recent deaths: [Peter Sutcliffe](#) · [Jerry Rawlings](#) · [Abdulkadir Balarabe Musa](#) · [Amadou Toumani Touré](#) · [Sven Wollter](#) · [Saeb Erekat](#)

[Other recent events](#) · [Nominate an article](#)

On this day

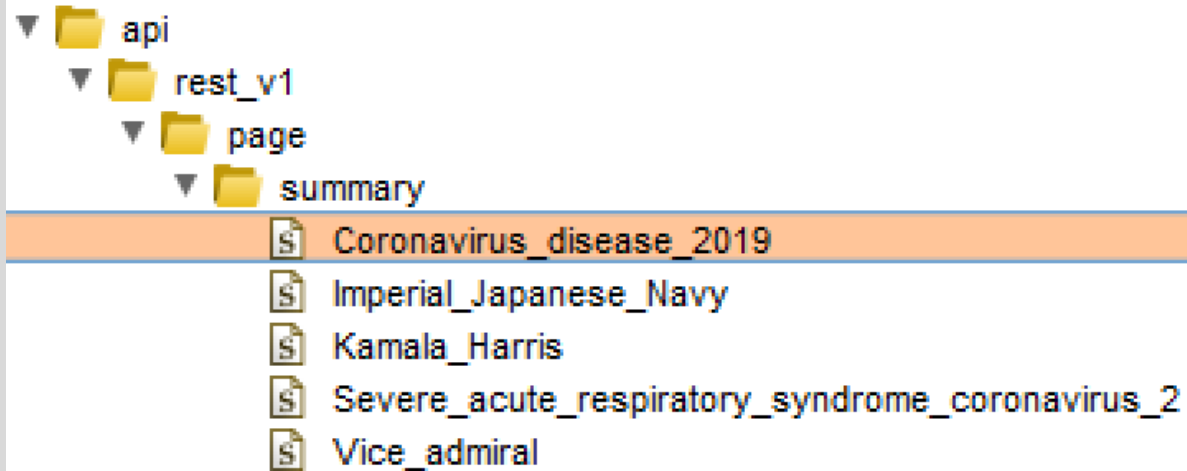
November 14: World Diabetes Day

- 1680 – German astronomer



CASE STUDY: Wikipedia

W U T ?



```
content-type: application/json; charset=utf-8;
profile="https://www.mediawiki.org/wiki/Specs/Summary/1.5.0"
access-control-allow-origin: *
access-control-allow-methods: GET,HEAD
access-control-allow-headers: accept, content-type, content-length, cache-control, accept-
language, api-user-agent, if-match, if-modified-since, if-none-match, dnt, accept-encoding
x-webkit-csp: default-src 'none'; frame-ancestors 'none'
x-request-id: 15190235-b01b-478d-bd0f-b77e5a53d4b1
server: restbase2009
```

1. Change in technology?
2. REST is not a Front Controller!
3. WHAT DOES IT MEAN!?
4. (most likely XFHR)
5. (because it is)

CASE STUDY: Wikipedia

W U T M O A R ?

Request

```
POST /beacon/event?%7B%22event%22%3A%7B%22action%22%3A%22ui-  
badge-link-  
click%22%2C%22version%22%3A%221.12%22%2C%22userId%22%3A%2240547119%  
2C%22editCount%22%3A%220%22%2C%22notificationType%22%3A%22message%22%7  
D%22%2C%22schema%22%3A%22EchoInteraction%22%2C%22webHost%22%3A%22  
en.wikipedia.org%22%2C%22wiki%22%3A%22enwiki%22%2C%22revision%22%3  
A15823738%7D; HTTP/1.1
```

Response

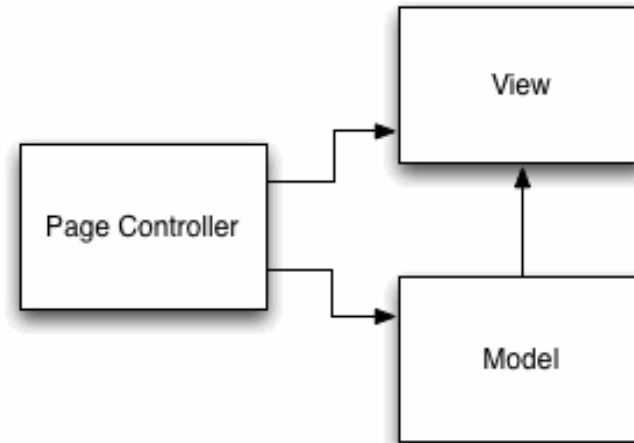
```
HTTP/1.1 204  
Date: Wed, 11 Nov 2020 06:27:17 GMT  
Server: Varnish  
X-Cache: cp4027 int  
X-Cache-Status: int-front  
Server-Timing: cache;desc="int-front"  
Strict-Transport-Security: max-age=106384710; includeSubDomains; preload
```

1. Another change in technology?
2. This isn't REST or a FRONT CONTROLLER!
3. Likely an interaction tracker
4. Maybe not a big deal

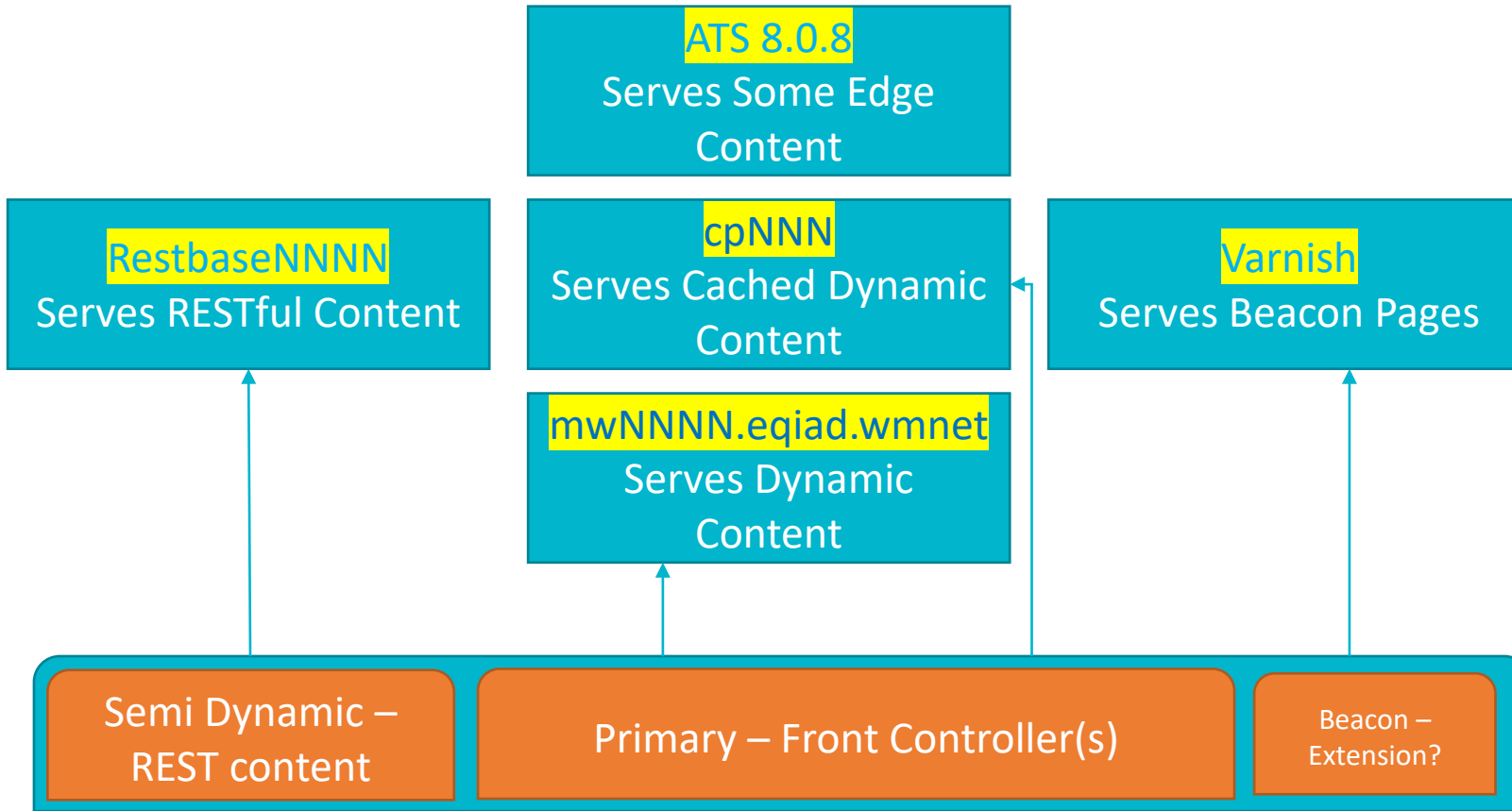
Page Controller Pattern

Web Presentation

1. The page is the controller. Everything to run it, all the logic is in that page.
2. Likely to have specific behaviours
3. Possibly inherits some base code from a shared source



Logging
- NEL



Ecommerce

 [Cart Functionality](#)

Wikis


 [MediaWiki](#)

Programming languages

php [PHP](#)

JavaScript libraries

 [jQuery UI](#) 1.9.2

 [Moment.js](#) 2.25.2

 [jQuery Migrate](#) 3.1.0

 [jQuery](#) 3.4.1

 [Create an alert for this website](#)



What did we learn? Wikipedia



1. Possible SSRF attacks via the pdf download functionality, as it is making requests on our behalf.
2. We'd want to look into Cache Poisoning and other HTTP based attacks as maybe ways to bypass auth / cache.
3. Map the other functions, see what pops as 'interesting.' Review parameters since we know their conventions? (export params and re-test)
4. Attack the logging service via 2nd order attacks

What did we learn?

1. Scientific Method still rules
2. Patterns rely on your ability to identify them.
3. Violations of 'standards' leads to ambiguity
4. Numerous code patterns creates unique opportunities



Thank You



@kuzushi
sensecurity.io