HTTP Route Busting

Enumerating Routes Instead of Directories

Hello!

I am Dejan Zelic

I am a Penetration Tester, Team Lead at EARLY WARNING®

You can find me at @dejandayoff or dejandayoff.com

Agenda

- Traditional Web Applications
- Modern Web Applications
- HTTP Routing
- Exceptions
- How to Test

Traditional Web Applications

Traditional Web Applications

```
/var/www/
└── dejandayoff.com
    ├── about.html
    ├── admin
    │   ├── dashboard.php
    │   └── index.php
    ├── contact.php
    └── index.html
```

Traditional Web Applications

`https://dejandayoff.com/admin/dashboard.php`

Traditional Web Applications

```
/var/www/
└── dejandayoff.com
    ├── about.html
    ├── admin
    │   ├── dashboard.php
    │   └── index.php
    ├── contact.php
    └── index.html
```

Traditional Web Applications

https://dejandayoff.com/admin/dashboard.php

Method = GET
Host = dejandayoff.com
Path = /admin/dashboard.php

Response: 200 OK

Traditional Web Applications

https://dejandayoff.com/admin/potato.php

Method = GET
Host = dejandayoff.com
Path = /admin/potato.php

Response: 404 Not Found

> *[Dirb] looks for existing Web Objects… by launching a dictionary based attack against a web server and analyzing the response*

Modern Web Applications

Modern Web Applications

https://dejandayoff.com/user/n0j

Modern Web Applications

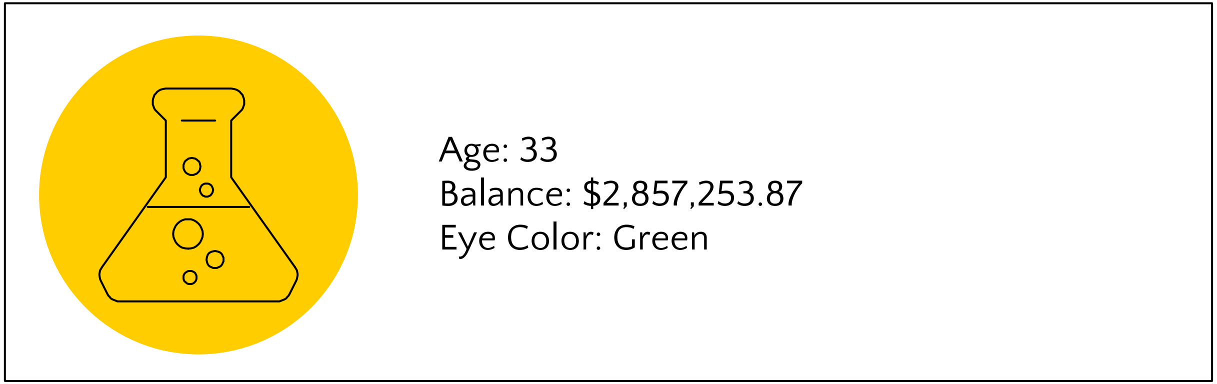
```
https://api.dejandayoff.com/user/n0j
```

Method = GET
Host = dejandayoff.com
Resource = /user/n0j

Modern Web Applications

```
https://api.dejandayoff.com/user/n0j
```

Response Code 200



Age: 33
Balance: $2,857,253.87
Eye Color: Green

Modern Web Applications

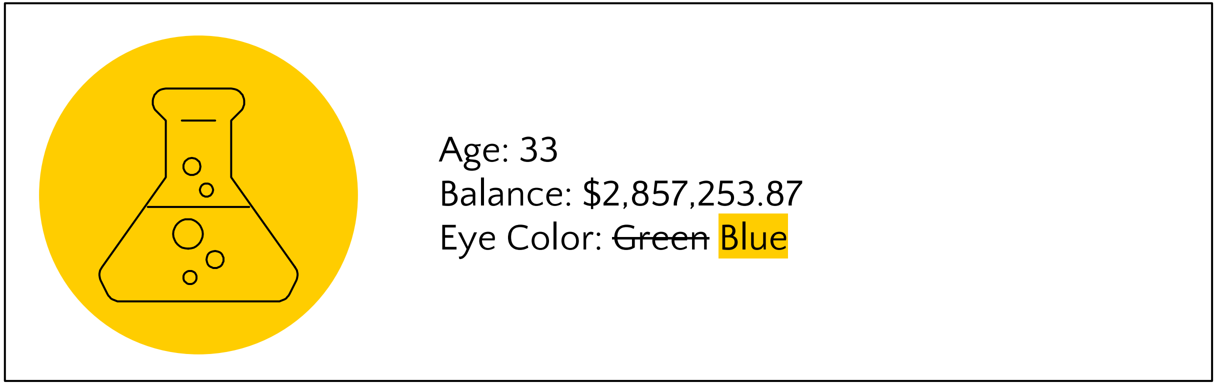
`https://api.dejandayoff.com/user/potato`

Response Code 404

Error “potato” is not found

Modern Web Applications

```
PUT https://api.dejandayoff.com/user/n0j
```



Age: 33
Balance: $2,857,253.87
Eye Color: ~~Green~~ Blue

Modern Web Applications

```
https://api.dejandayoff.com/user/hackerbyhobby
https://api.dejandayoff.com/user/n0j
https://api.dejandayoff.com/user/bruteforce1
https://api.dejandayoff.com/user/1N3
https://api.dejandayoff.com/user/AV-IO
https://api.dejandayoff.com/user/sudo-phantom
https://api.dejandayoff.com/user/broadcast
https://api.dejandayoff.com/user/beastmaster90
```

Modern Web Applications

https://api.dejandayoff.com/user/hackerbyhobby

200 - ✓

https://api.dejandayoff.com/user/

404 - ✗

HTTP Routing

HTTP Routing

```
app.get('/user/:name', function(req, res){
    res.render('user', req.params.name);
});
```

Modern Web Applications

```
Modern Application:
https://dejandayoff.com/user/n0j

Traditional Application:
https://dejandayoff.com/user.php?name=n0j
```

HTTP Routing

```
app.get('/user/:name', function(req, res){
    res.render('user', req.params.name);
});
```

HTTP Routing

```
app.post('/user/:name', function(req, res){
    create(req.params.name, req.body);
});
```

HTTP Routing

```
app.put('/user/:name', function(req, res){
    update(req.params.name, req.body);
});
```

HTTP Routing

```
app.delete('/user/:name', function(req, res){
    delete(req.params.name);
});
```

Exceptions

Exceptions

https://dejandayoff.com/user/hackerbyhobby

https://dejandayoff.com/index.php/user/hackerbyhobby

Exceptions

https://dejandayoff.com/css/

https://dejandayoff.com/js/

https://dejandayoff.com/img/

https://dejandayoff.com/vendor/

How to Test

How would I test Modern Applications any differently than I would Traditional Applications.

Whitebox Approach

Whitebox Approach

Drupal 8 – .routing.yml

Wordpress – register_rest_route()

Joomla – router.php

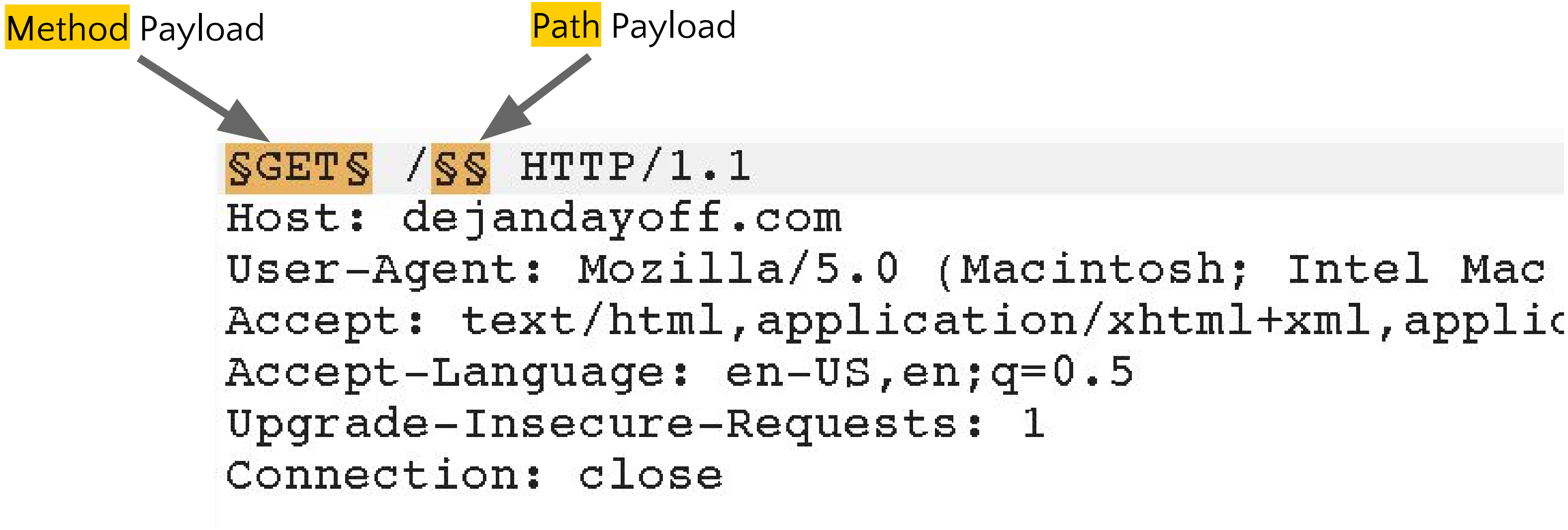
Node (express) – app.get(), app.put(), etc.

Rails – get "users", to: "users#index"

Symfony – routing.yml, routing.xml, routing.php

Blackbox Approach

Blackbox Approach



Method Payload

Path Payload

```
§GET§ /§§ HTTP/1.1
Host: dejandayoff.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac
Accept: text/html,application/xhtml+xml,applic
Accept-Language: en-US,en;q=0.5
Upgrade-Insecure-Requests: 1
Connection: close
```

Blackbox Approach

Method Payloads:

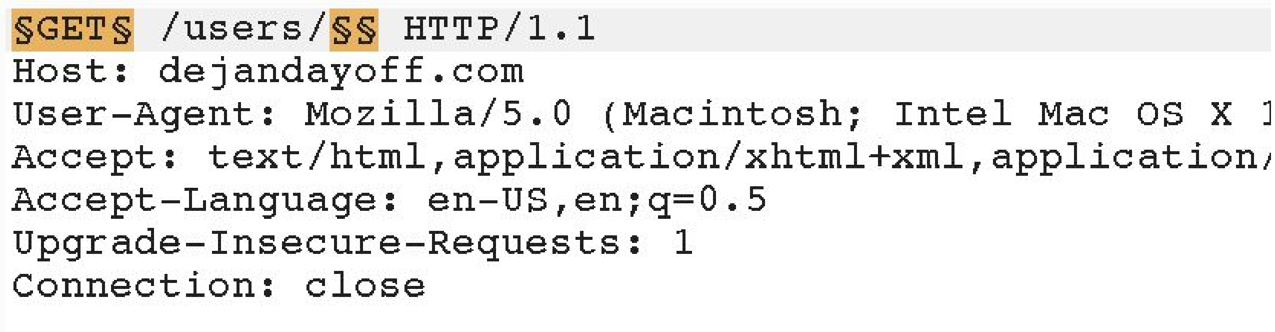
- GET
- PUT
- POST
- DELETE
- ...

Blackbox Approach

Path Payloads:

- Dirb common.txt is ok
- Depends…
  - /users/

Blackbox Approach



```
§GET§ /users/§§ HTTP/1.1
Host: dejandayoff.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 1
Accept: text/html,application/xhtml+xml,application/
Accept-Language: en-US,en;q=0.5
Upgrade-Insecure-Requests: 1
Connection: close
```

Take Away

- Sites are more “clean”
- Don’t blindly fuzz
- Understand the application
- Don’t assume using GET will find everything
  - Brute force the methods

Thanks!

Any *questions* ?

You can find me at

- @dejandayoff
- dejandayoff.com

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival