



ความปลอดภัยคอมพิวเตอร์ (424) OWASP : เวลัยโงทัย ★ เดียว

สำหรับนักศึกษาชั้นปีที่ 4 สาขาวิชาวิศวกรรมคอมพิวเตอร์

กรุงฤทธิ์ กิติศรีวงศ์พันธุ์
Email : songrit@npu.ac.th
สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยนครพนม

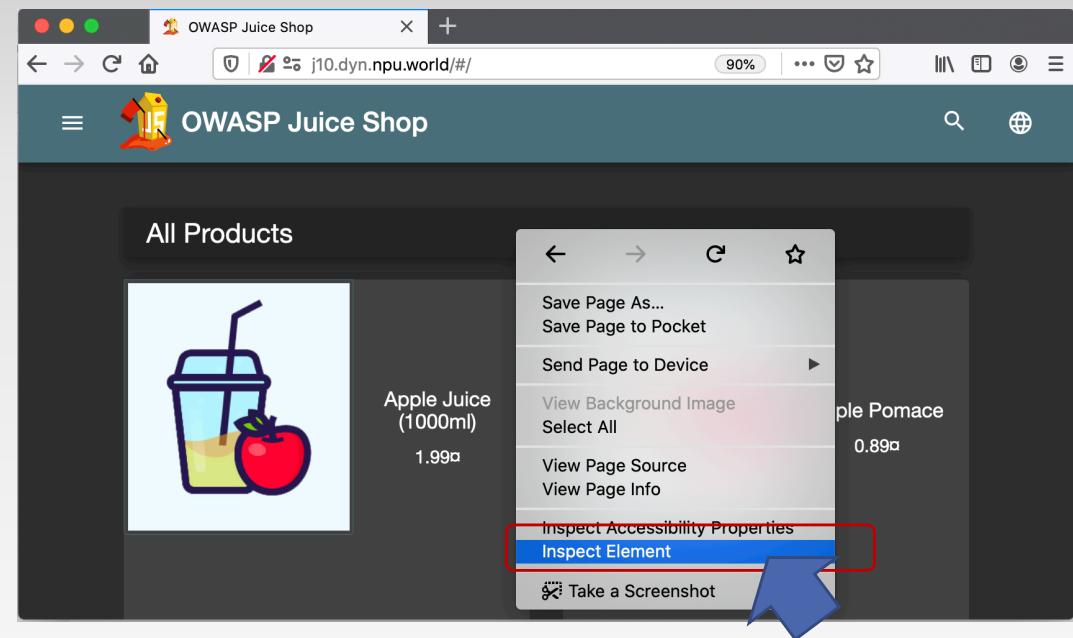
Revised 2020-10-04

Agenda Level :

Name	Description
Score Board	หน้าเพ็จ "Score Board"
Privacy Policy	Read our privacy policy.
DOM XSS	Perform a <i>DOM XSS</i> attack with <iframe src="javascript:alert('xss')">.
Bonus Payload	Use the bonus payload .. in the <i>DOM XSS</i> challenge.
Bully Chatbot	Receive a coupon code from the support chatbot.
Confidential Document	เข้าถึงไฟล์เอกสารลับ
Error Handling	Provoke an error that is neither very gracefully nor consistently handled.
Exposed Metrics	Find the endpoint that serves usage data to be scraped by a popular monitoring system .
Missing Encoding	Retrieve the photo of Bjoern's cat in "melee combat-mode".
Outdated Whitelist	Let us redirect you to one of our crypto currency addresses which are not promoted any longer.
Repetitive Registration	Follow the DRY principle while registering a user.
Zero Stars	ให้คะแนนร้านค้า 0 ดาว

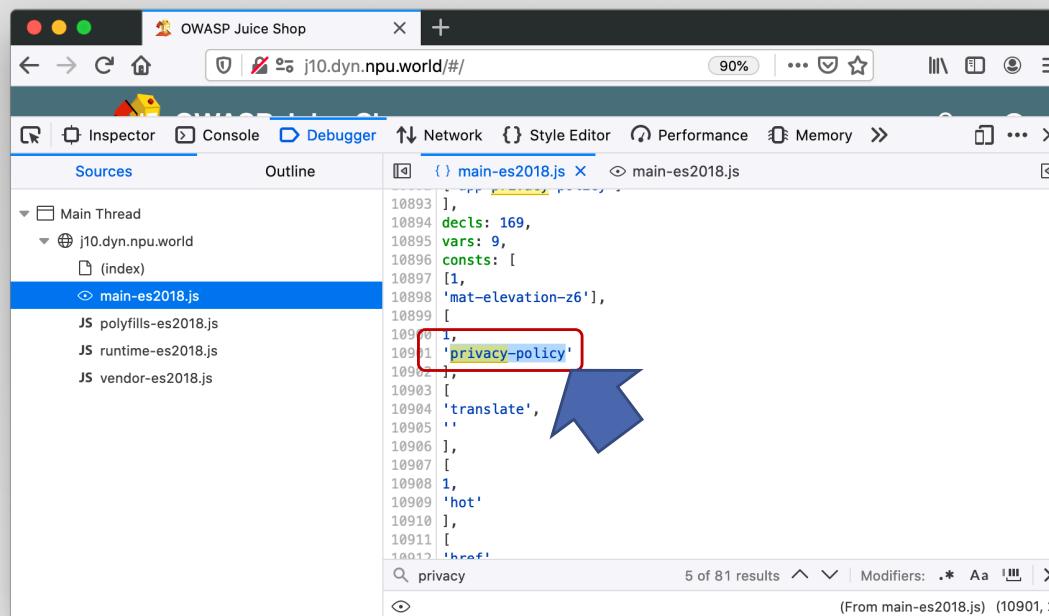
Score Board

- ค้นหาเพ็จ score board
- ใช้เครื่องมือสำหรับนักพัฒนาจาก Browser
- กดเว็บแล้วสังเกต URL หลังเครื่องหมาย #
- URL มีการตรวจสอบด้วย Javascript
- ค้นหาคำเกี่ยวกับ score board



Privacy Policy

- ใช้ Web inspector ค้นหา URL เกี่ยวกับ privacy



```
10893 ],
10894     decls: 169,
10895     vars: 9,
10896     consts: [
10897     [1,
10898     'mat-elevation-z6'],
10899     [
10900     ],
10901     'privacy-policy'
10902     ],
10903     [
10904     'translate',
10905     ''
10906     ],
10907     [
10908     1,
10909     'hot'
10910     ],
10911     [
10912     'href'
10913 ]]
```

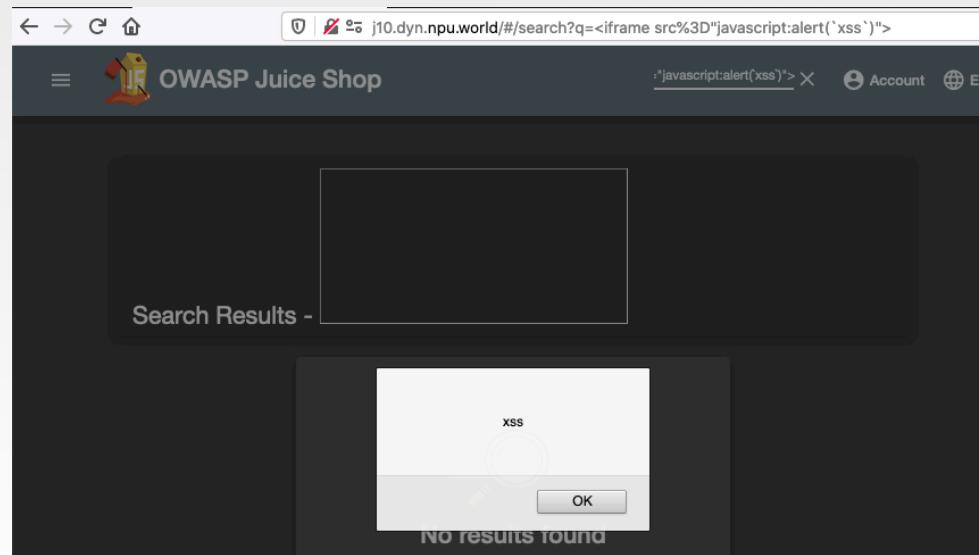
privacy

5 of 81 results

(From main-es2018.js) (10901, 2)

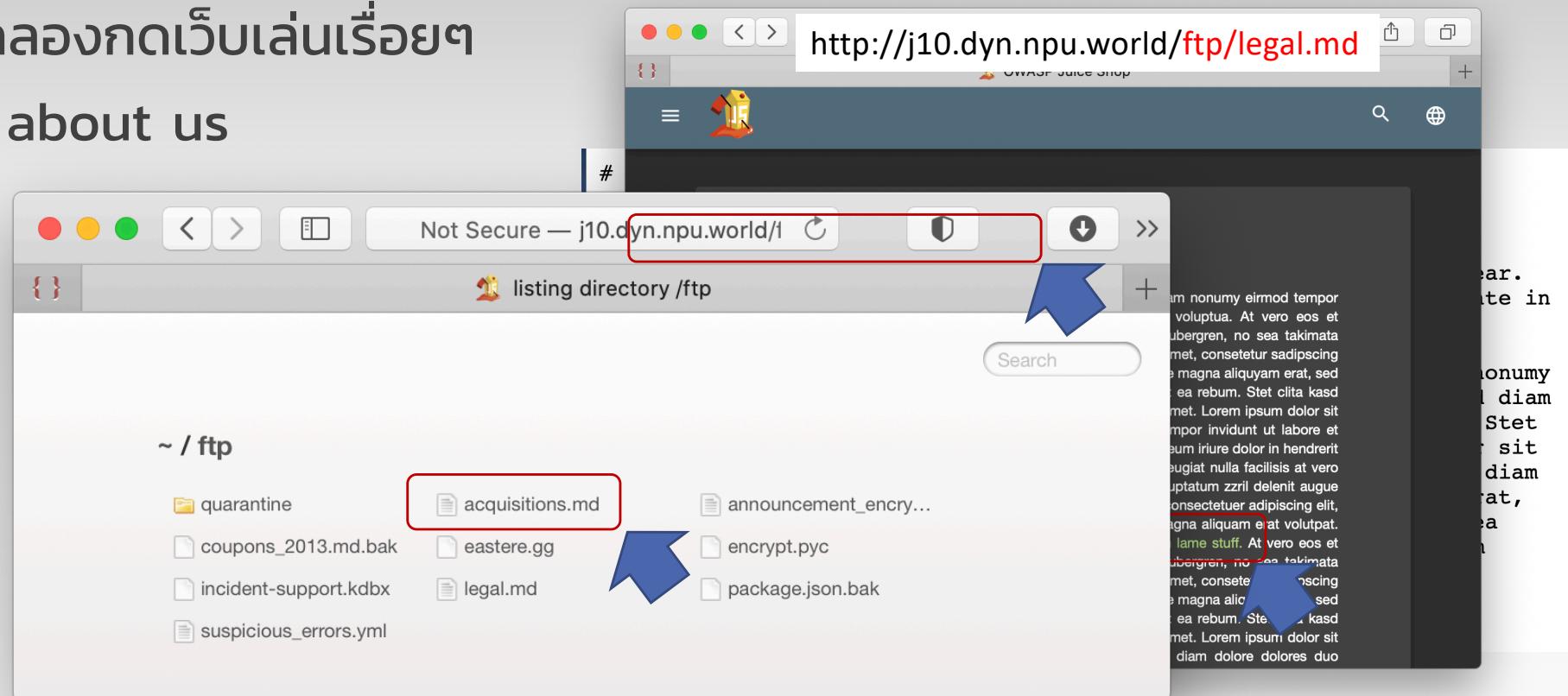
DOM XSS

- รับ Cross site scripting
- ค้นหาช่องรับข้อมูล กดสอบสั่ง html tag
- ใช้ คำสั่งที่โจทย์ให้มา
 - <iframe src="javascript:alert('xss')">



Confidential Document

- หลังจากลองกดเว็บเล่นเรื่อยๆ
- เข้าหน้า about us



Exposed Metrics

- เว็บ Monitor ระบบ มีไว้สำหรับผู้ดูแลระบบ แต่เมื่อเก็บไม่ในตำแหน่งไม่ปลอดภัยจะถูกลักลอบอ่านข้อมูล
- จากโจทย์ลิงค์ไปที่ <https://github.com/prometheus/prometheus>
- การติดตั้งโปรแกรม
 - https://prometheus.io/docs/introduction/first_steps/

Starting Prometheus

To start Prometheus with our newly created configuration file, change to the directory containing the Prometheus binary and run:

```
./prometheus --config.file=prometheus.yml
```

Prometheus should start up. You should also be able to browse to a status page about itself at <http://localhost:9090>. Give it about 30 seconds to collect data about itself from its own HTTP metrics endpoint.

You can also verify that Prometheus is serving metrics about itself by navigating to its own metrics endpoint:
<http://localhost:9090/metrics>.



Bonus Payload

- ส่ง XSS ผ่าน URL โดยตรง
- แปลง โค้ดให้อยู่ในรูปแบบ URL
- <https://meyerweb.com/eric/tools/dencoder/>
- <https://www.url-encode-decode.com>

The screenshot shows two side-by-side code editors. The left editor contains the following HTML code:

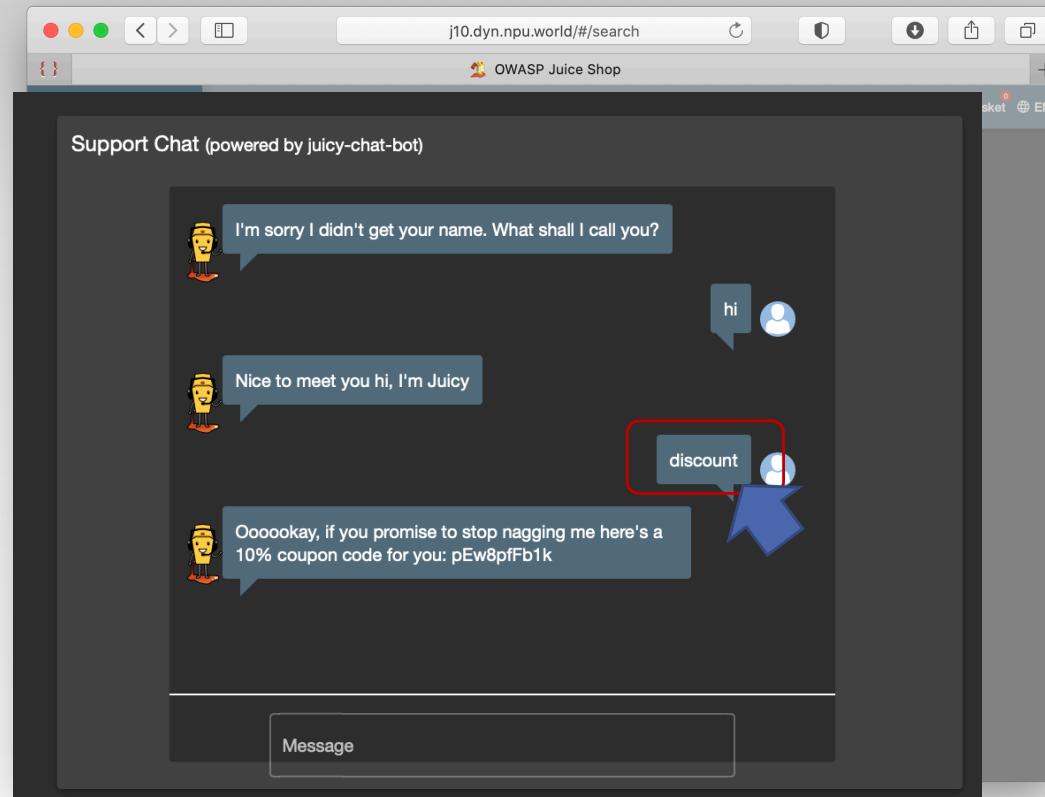
```
<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A/api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>
```

The right editor shows the URL-encoded version of the same code, which has been converted by the dencoder tool. A red box highlights the encoded URL, and a blue arrow points from the left editor to the right editor.

→ Encode url ← Decode url Start Over

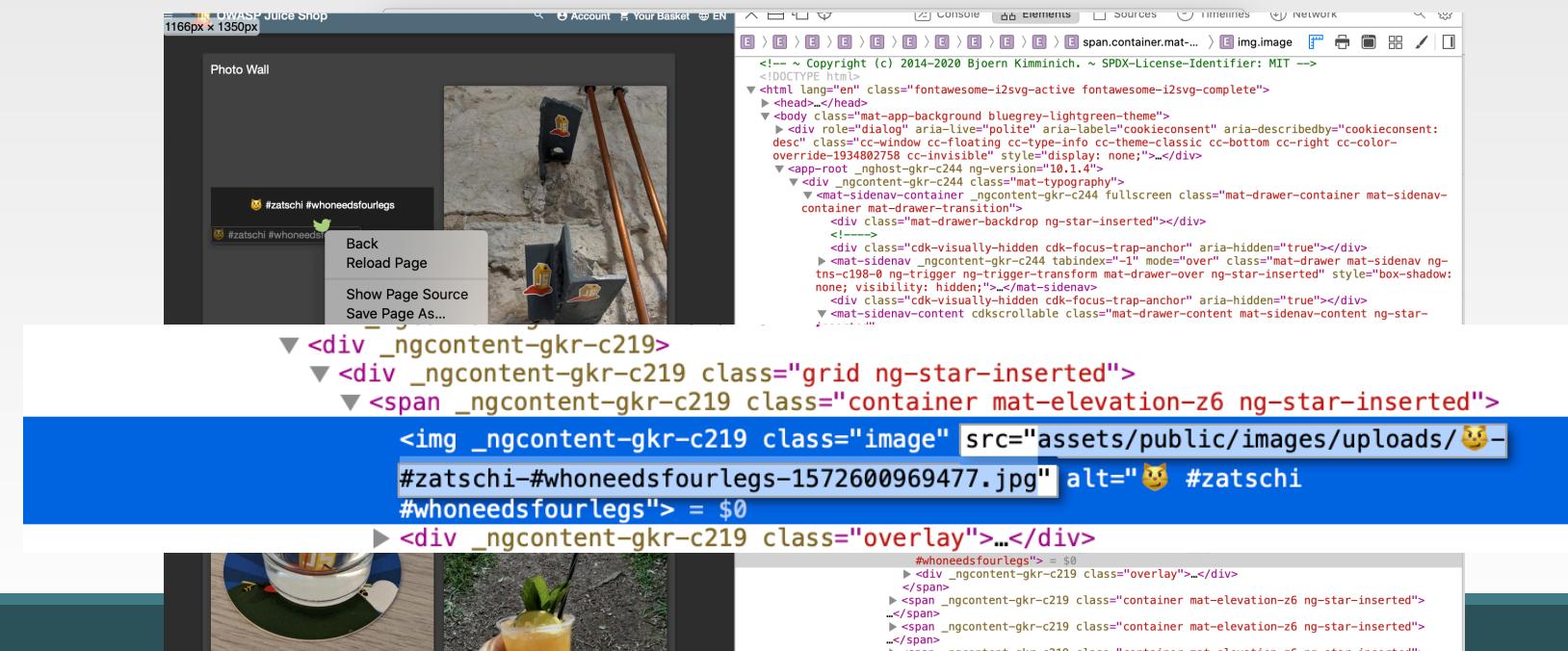
Bully Chatbot

- ขอคุปองส่วนลดกับ Chatbot
- Login ด้วย user ใดๆ
- เลือก chatbot
- ทักทายบอท
- ถามขอบัตรส่วนลด



Missing Encoding

- ค้นหารูปแมวของ Bjoern
- <http://j10.dyn.npu.world/#/photo-wall>
- เมื่องคไม่สมบูรณ์ --> ใช้ URL encoder



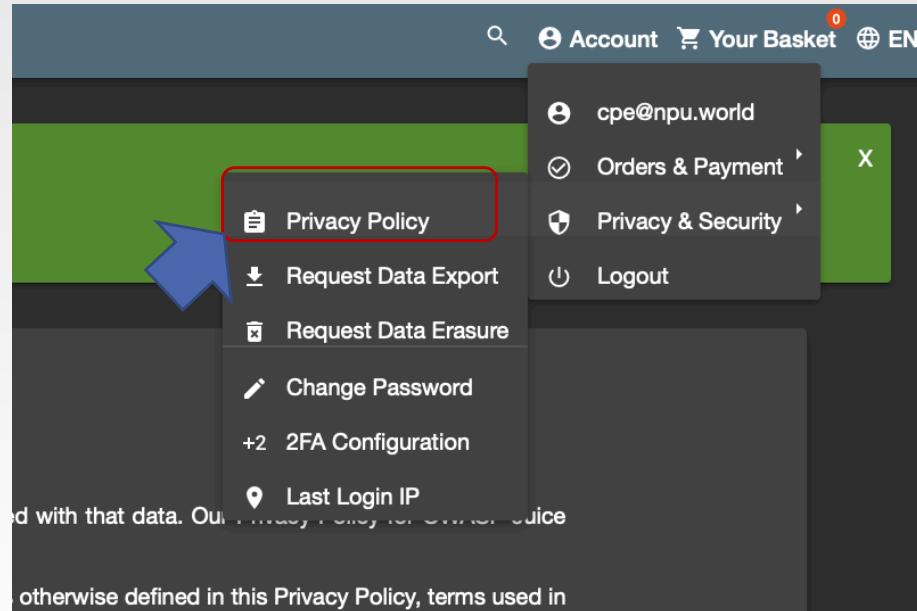
Outdated Whitelist

- มีสิ่งค์เก่าที่แอดมินลืมลบ เป็น bitcoin address ของร้าน
- ก่อนนี้ร้านเคยใช้ bitcoin ปัจจุบันเลิกใช้ แต่ไม่ได้ลบข้อมูลเก่า
- ค้นหาในไฟล์ main-es2018.js
- ./redirect?to=https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm

```
6595 console.log(t),
6596     this.snackBarHelperService.open(null === (e
6597 = t.error) || void 0 === e ? void 0 : e.error, "errorBar")
6598     }, "deluxe" === this.mode ?
6599     this.userService.upgradeToDeluxe(this.paymentMode).subscribe(t => {
6600         localStorage.setItem("token", t.token),
6601         this.cookieService.set("token", t.token),
6602         this.ngZone.run(() =>
6603             this.router.navigate(["/deluxe-membership"]))
6604         }, t => console.log(t)) : ("wallet" ===
6605         this.paymentMode ? sessionStorage.setItem("paymentId", "wallet") :
6606         sessionStorage.setItem("paymentId", this.paymentId), this.ngZone.run()
6607 => this.router.navigate(["/order-summary"])))
6608     )
6609     noop() {}
6610     showBitcoinQrCode()
6611     {
6612         this.dialog.open(Pn, {
6613             data: {
6614                 data:
6615                 "bitcoin:1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
6616                 url: "./redirect?"
6617                 to="https://blockchain.info/address/1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
6618                 address:
6619                 "1AbKfgvw9psQ41NbLi8kufDQTezwG8DRZm",
6620                 title: "TITLE_BITCOIN_ADDRESS"
6621             }
6622         })
6623         showDashQrCode()
6624         {
6625             this.dialog.open(Pn, {
6626                 data: {
6627                     data:
6628                     "dash:Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW",
6629                     url: "./redirect?"
6630                     to="https://explorer.dash.org/address/Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW
6631                     ",
6632                     address:
6633                     "Xr556RzuwX6hg5EGpkybbv5RanJoZN17kW",
6634                     title: "TITLE_DASH_ADDRESS"
6635             })
6636         }
6637     }
6638 }
```

Read our privacy policy

- อ่านนโยบายด้าน Privacy ของเว็บ
- login → เลือก Account → Privacy & Security



Repetitive Registration

- ใช้แนวคิด DRY(Don't Repeat Yourself)
ลงทะเบียนผู้ใช้
- ป้อนรหัสผ่านแรก
- แล้วป้อนรหัสผ่านที่ช่อง Repeat Password
- ลองกลับไปเปลี่ยนรหัสผ่านที่ช่องแรก
พบว่าระบบตรวจสอบทำงานผิดพลาด

User Registration

Email
test@test.com

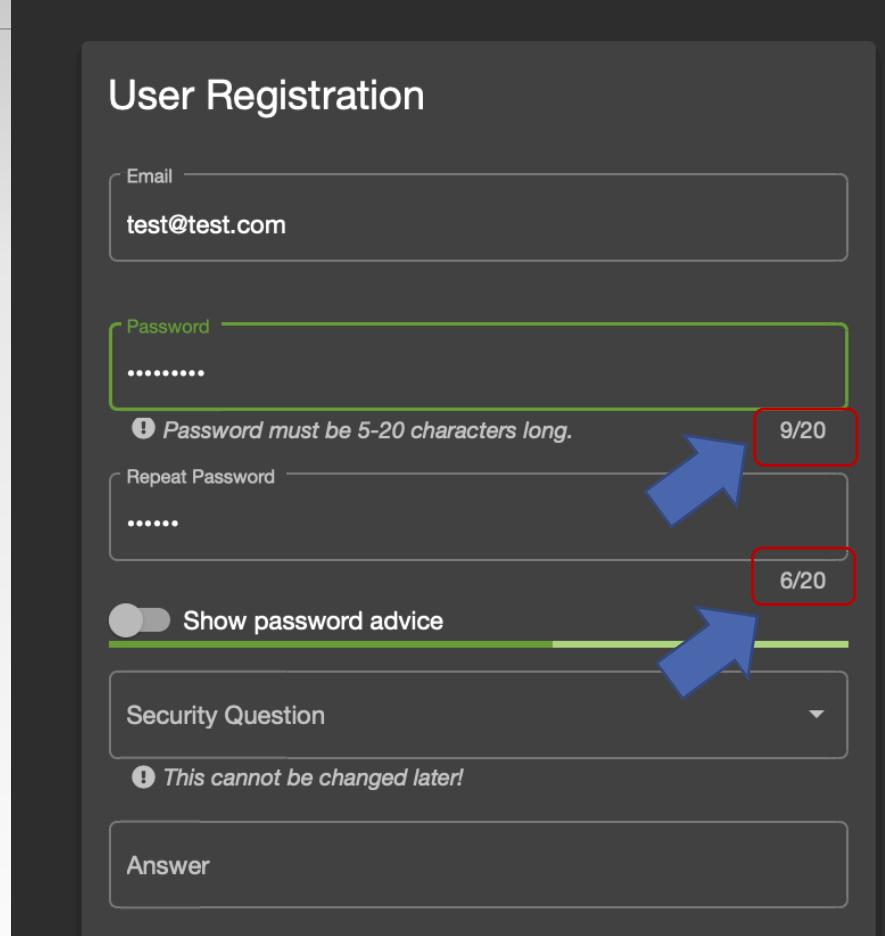
Password
.....
>Password must be 5-20 characters long. 9/20

Repeat Password
..... 6/20

Show password advice

Security Question
This cannot be changed later!

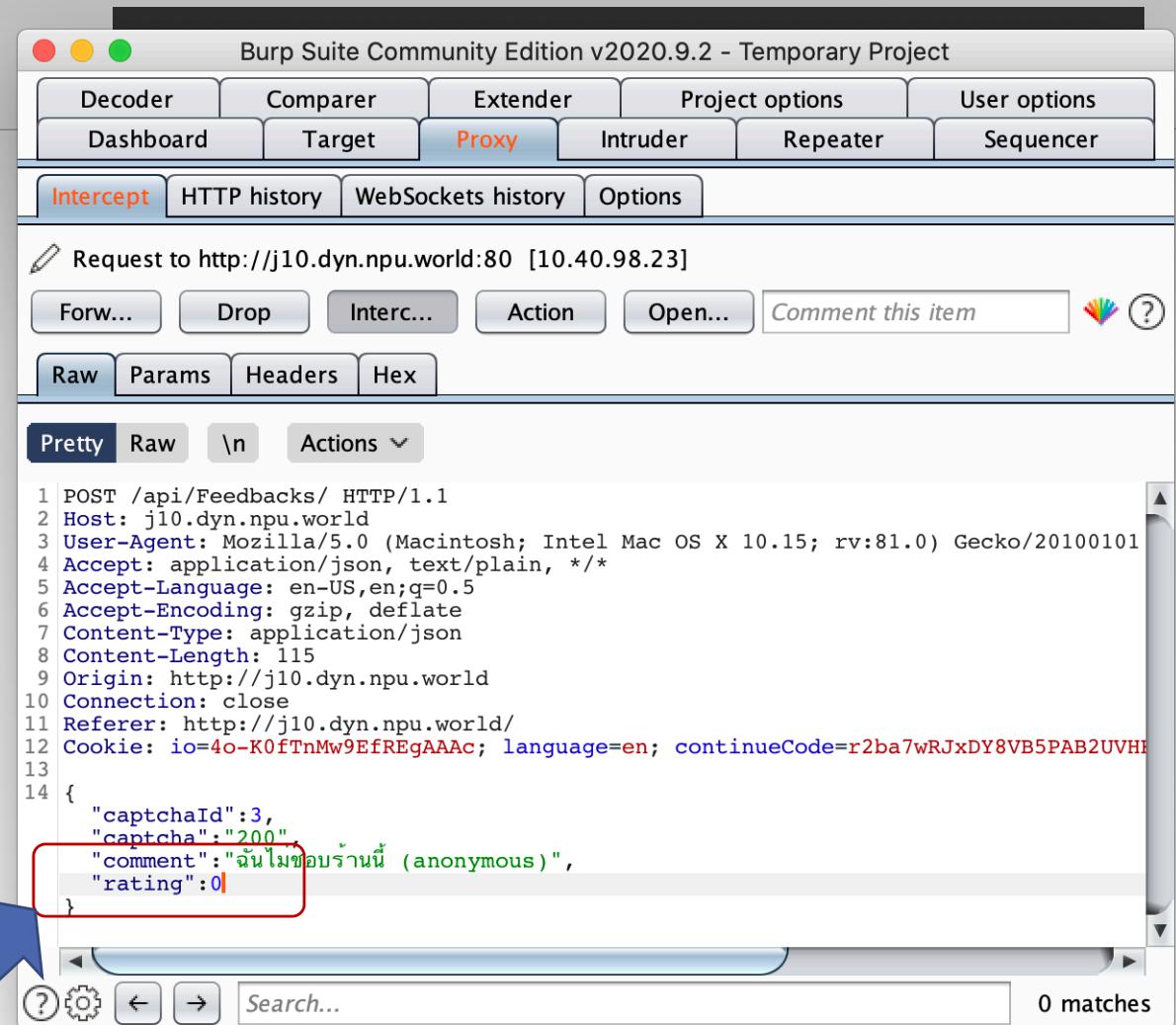
Answer



The screenshot shows a dark-themed user registration interface. At the top, it says "User Registration". Below that is an "Email" field containing "test@test.com". Underneath is a "Password" field with a green border and a red box highlighting the character count "9/20". A blue arrow points from the text "Repeat Password" to this field. Below the password field is a "Repeat Password" field with a character count of "6/20". Another blue arrow points from the "Show password advice" toggle switch to this field. Further down is a "Security Question" dropdown menu with a note "This cannot be changed later!". At the bottom is an "Answer" field.

Zero Stars

- ให้ feedback 0
- เว็บให้ใส่ได้น้อยสุด 1 ดาว แต่เราจะให้ 0 ดาว



Burp Suite Community Edition v2020.9.2 - Temporary Project

Decoder Comparer Extender Project options User options

Dashboard Target Proxy Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

Request to http://j10.dyn.npu.world:80 [10.40.98.23]

Forw... Drop Interc... Action Open... Comment this item

Raw Params Headers Hex

Pretty Raw \n Actions ▾

```
1 POST /api/Feedbacks/ HTTP/1.1
2 Host: j10.dyn.npu.world
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:81.0) Gecko/20100101
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Content-Length: 115
9 Origin: http://j10.dyn.npu.world
10 Connection: close
11 Referer: http://j10.dyn.npu.world/
12 Cookie: io=4o-K0fTnMw9EfREgAAAc; language=en; continueCode=r2ba7wRJxDY8VB5PAB2UVH
13
14 {
    "captchaId":3,
    "captcha":"200",
    "comment": "ฉันไม่ขอเป็นร้านนี้ (anonymous)",
    "rating":0
}
```

0 matches