BAB 4
HASIL PENELITIAN

4.1 RINGKASAN HASIL PENELITIAN

Penelitian ini bertujuan untuk mengukur keamanan Sistem Informasi pada Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta dengan metode penetration testing yang hasilnya nanti bisa menjadi bahan evaluasi terkait keamanan yang ada didalamnya. Dengan izin yang telah didapatkan untuk melakukan pengujian terhadap Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta. Dengan menggunakan *tools* yang ada pada Kali Linux, terdapat sebuah informasi *senstive, vulnerability* dan dari masing – masing hal tersebut beresiko terkena *attack* jika tidak diketahui oleh pihak pemilik. Dari hasil pengujian yang dilakukan pada Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta memberikan data pengujian yang dilakukan pada *landing page* tingkat kerentanan berada pada *level medium*, pada *web app* (mahasiswa) tingkat kerentanan berada pada level critical dan assement pada penelitian ini terhadap website Sistem Informasi Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta tingkat kerentanan berada di *level medium*.

4.2 PEMBAHASAN

4.2.1 Pre - engagement

Pada tahap ini proses penetration testing yang dilakukan penguji adalah mempersiapkan peralatan dan teknik, merancang jadwal pengujian, koordinasi projek, mempersiapkan dokumen yang berupa perizinan studi kasus penelitian yang diserahkan kepada pihak Universitas Jenderal Achmad Yani Yogyakarta.

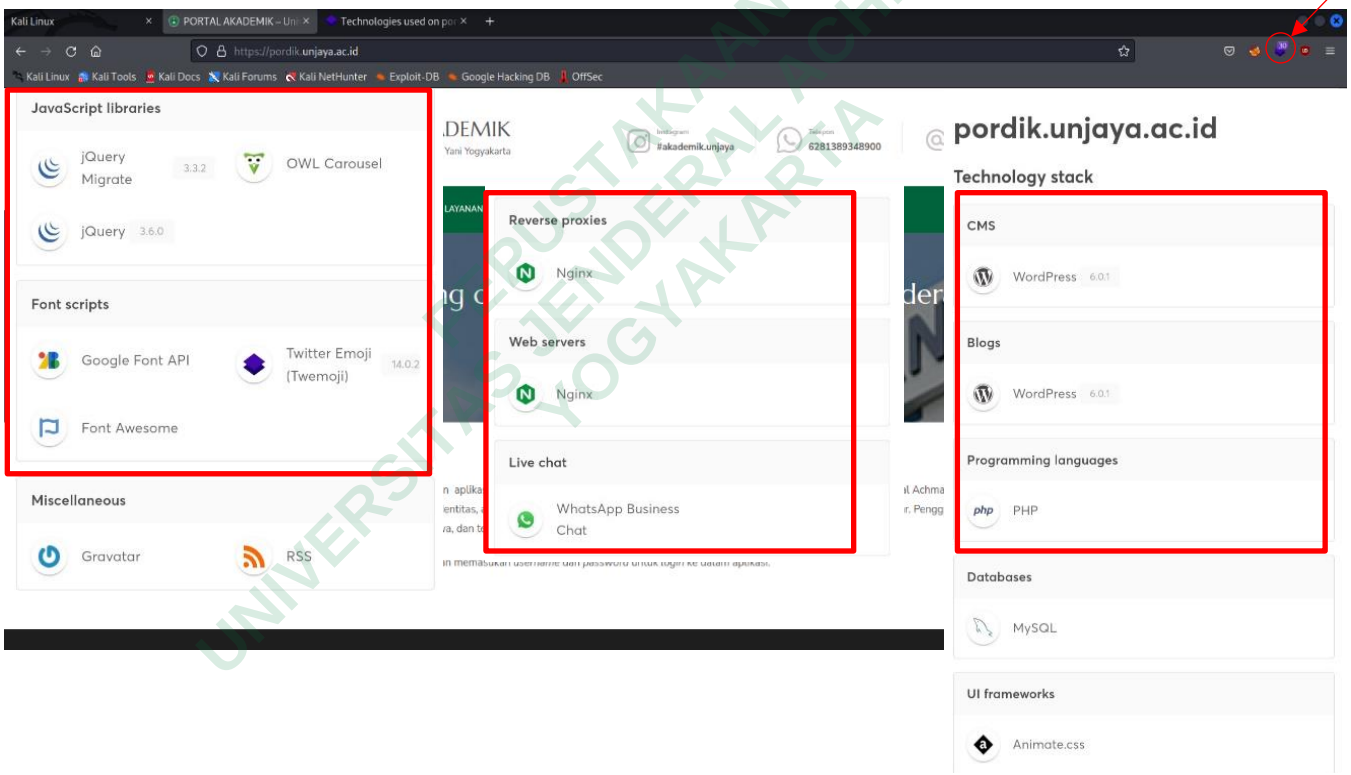
4.2.2 Reconnaisance

Pada proses melakukan *recconnaisance,* penguji/peneliti melakukan 2 tahapan yaitu, tahapan *reconnaisance* secara pasif dan tahapan *reconnaisance* secara aktif.

4.2.2.1 Passive Reconnaissance

Passive reconnaissance merupakan pengumpulan informasi dan data mengenai objek atau target yang akan diteliti tanpa langsung berinteraksi dengan objek,layanan atau target yang akan diteliti. Pada tahapan *passive reconnaissance* biasanya informasi yang didapatkan masih bersifat umum. Kemudian *tools* yang digunakan pada *passive reconnaissance* menggunakan *search engine* yang berisikan *database* sistem yang sudah teranalisa. Berikut hasil dari tahapan *passive reconnasiance:*

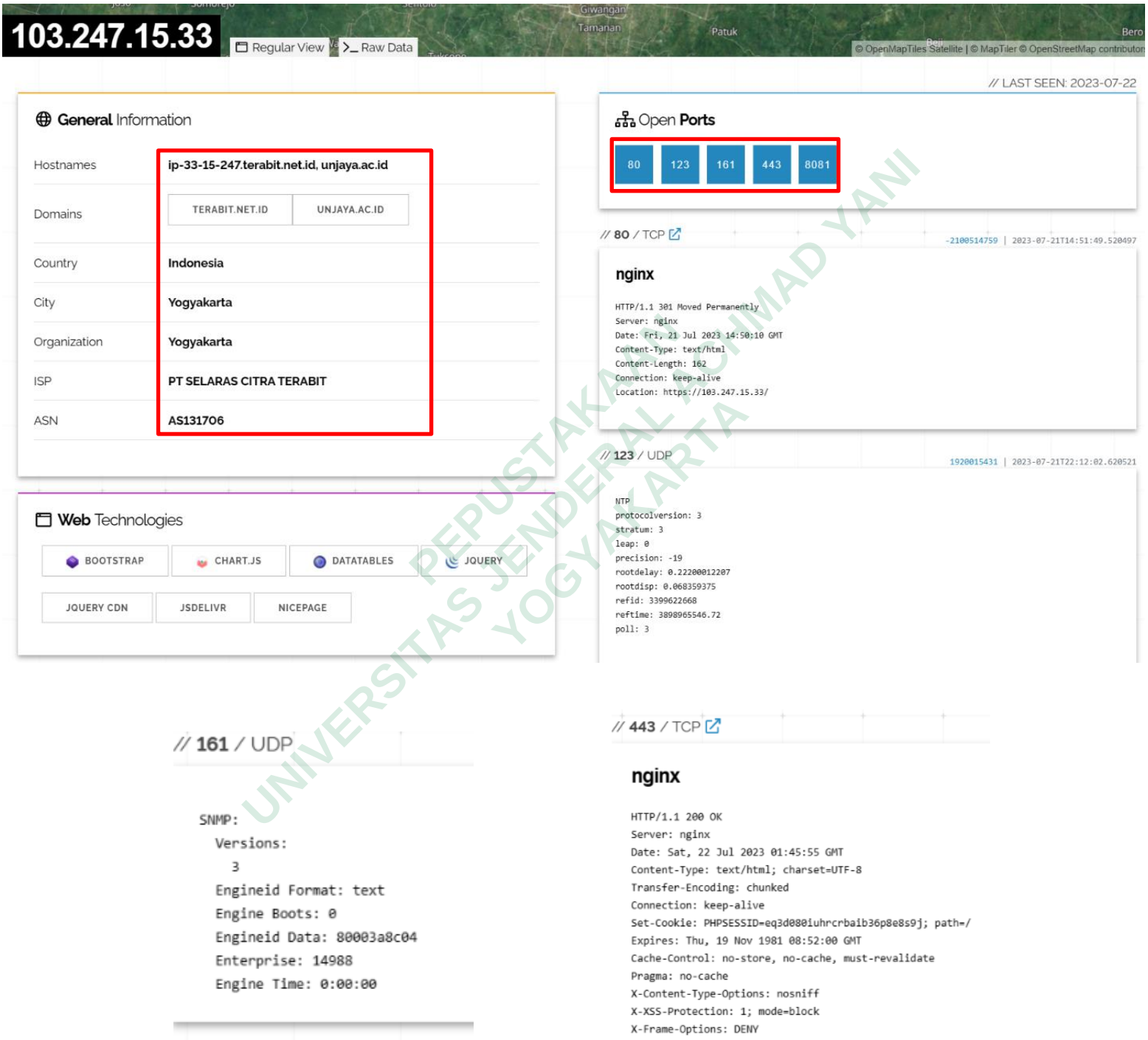
A. Mencari teknologi yang digunakan pada objek penelitian menggunakan *Wappalyzer*



Gambar 4.1 Informasi Arsitektur Objek Penelitian WappalyzerTools

Pada hasil seperti yang ditujukan pada Gambar 4.1 ditemukan teknologi yang digunakan pada objek penelitian menggunakan CMS WordPress, *databases* yang digunakan menggunakan MySQL, *web servers* menggunakan Nginx, Bahasa pemrograman menggunakan PHP.

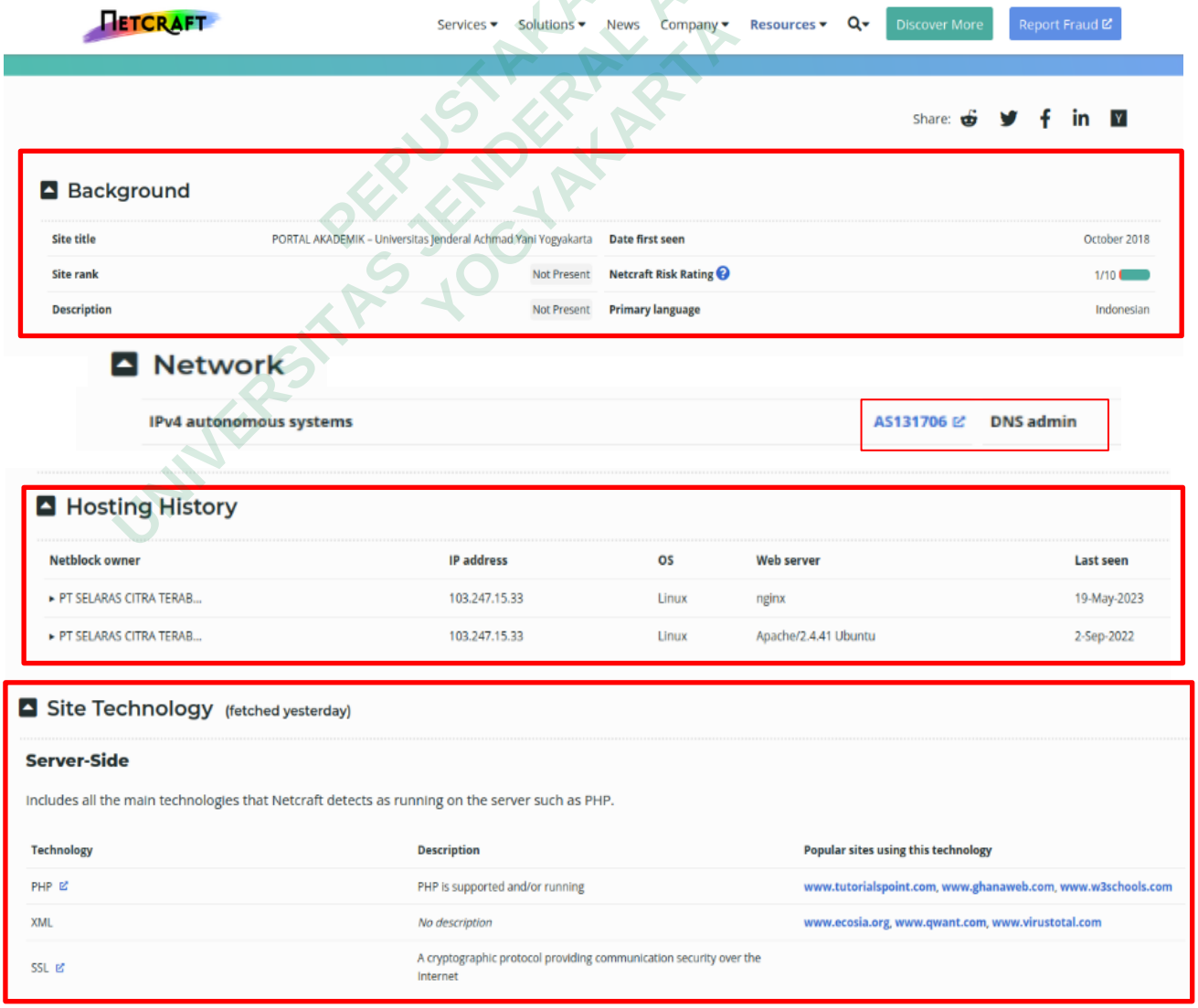
B. Mencari informasi kemanan jaringan, mengidentifikasi port yang tersedia pada sebuah objek, layanan target menggunaka search engine Bernama Shodan



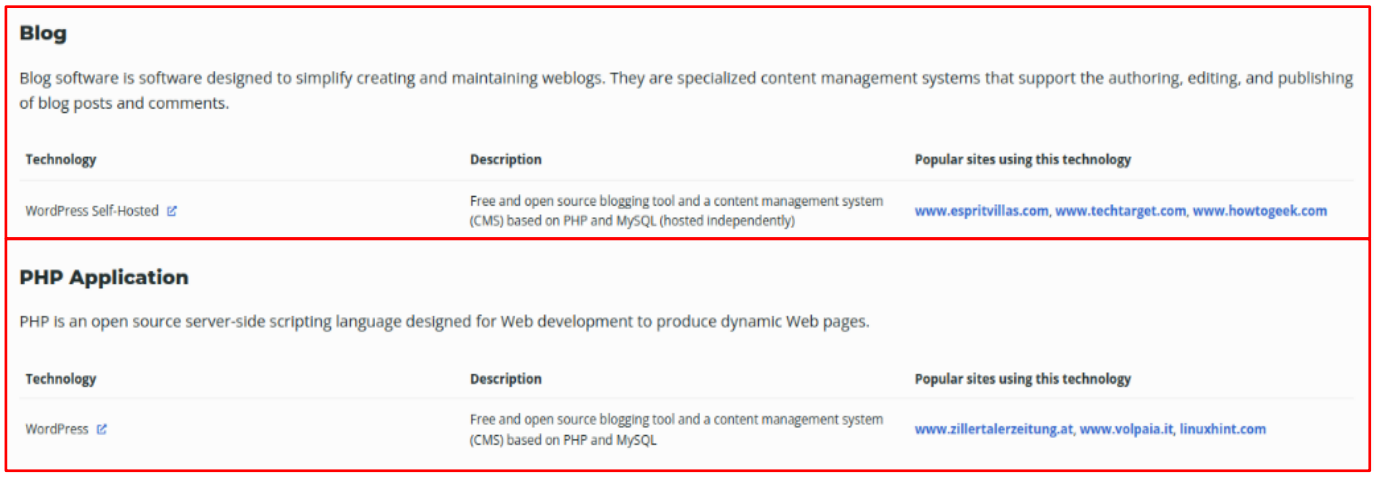
Gambar 4.2 General Information, Open Port Objek Penelitian Shodan Tools

Pada penggunaan *tools* Shodan yang ditujukan pada Gambar 4.2 ditemukan sebuah hasil, dimana alamat IP dan domain pada Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta ISP (*Internet Service Provider*) menggunakan layanan dari PT SELARAS CITRA TERABIT. Terdapat informasi port yang digunakan pada layanan Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta yaitu: port 80 (TCP), port 123 (UDP),port 161 (UDP), port 443 (TCP).

C. Melakukan proses reconnaisnce *web server*, sistem informasi, *hosting provider*, ISP, transaksi enkripsi, bisnis secara elektronik (*web server survey*) menggunakan *Netcraft* seperti yang ditujukan pada Gambar 4.3 dan Gambar 4.4



Gambar 4.3 Informasi Background, Hosting History,Site Technology Objek Penelitian Netcraft Tools



Blog

Blog software is software designed to simplify creating and maintaining weblogs. They are specialized content management systems that support the authoring, editing, and publishing of blog posts and comments.

Technology	Description	Popular sites using this technology
WordPress Self-Hosted	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL (hosted independently)	www.espritvillas.com, www.techtarget.com, www.howtogeek.com

PHP Application

PHP is an open source server-side scripting language designed for Web development to produce dynamic Web pages.

Technology	Description	Popular sites using this technology
WordPress	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL	www.zillertalerzeitung.at, www.volpaia.it, linuxhint.com

Gambar 4.4 Informasi Teknologi Pada Blog dan Web Browser Targeting Objek Penelitian Netcraft Tools

Berdasarkan penggunaan *tools* netcraft diatas, ditemukan sebuah informasi atau data yang diletakan pada bagian bagian yang penting. Berikut penjelasan mengenai bagian tersebut:

a. Informasi atau data penting pertama pada bagian 1 mengenai background pada objek penelitian. Pada bagian background informasi atau data yang ditampilkan dari *tools* netcraft adalah
b. mengenai *Site tittle*, Data *first seen*, dan Netcraft *risk rating*. Untuk isi data 1 mengenai *site title* pada objek penelitian menggunakan nama PORTAL AKADEMIK – Universitas Jenderal Achmad Yani Yoyakarta. Isi data ke 2 mengenai data first seen pada objek penelitian ditampilkan bahwa data terakhir dilihat pada tahun 2018. Isi data ke 3 mengenai Netcraft *risk rating* pada objek penelitian menunjukan hasil 1/10 dari tingkat keamanan dan resiko, yang maknanya situs atau layanan dari objek penelitian terdapat sebuah keamanan untuk mengurangi resiko adanya serangan.
c. Informasi atau data penting ke dua pada bagian 2 mengenai *network* pada objek penelitian. Pada bagian network terdapat infromasi yang perlu dianalisa lebih lanjut yaitu, mengenai Virus total.
d. Informasi atau data penting ke tiga bagian 3 mengenai *hosting history* pada objek penelitian. Pada bagian *hosting history* terdapatat informasi pemilik *netblock (netblock owner)* dari

objek penelitian adalah PT SELARAS CITRA TERABIT. Kemudian IP *(internet protocol)* pada objek penelitian beralamatkan 103.247.15.33. Operating system yang digunakan adalah Linux. *Web server* yang digunakan pada objek penelitian adalah Nginx dan Apache/2.4.4.1 Ubuntu.

e. Informasi atau data ke empat bagian 4 mengenai *site technology* pada objek penelitian. Pada sisi server terdapat informasi mengenai keamanan yang digunakan yaitu menggunakan pengamanan SSL.

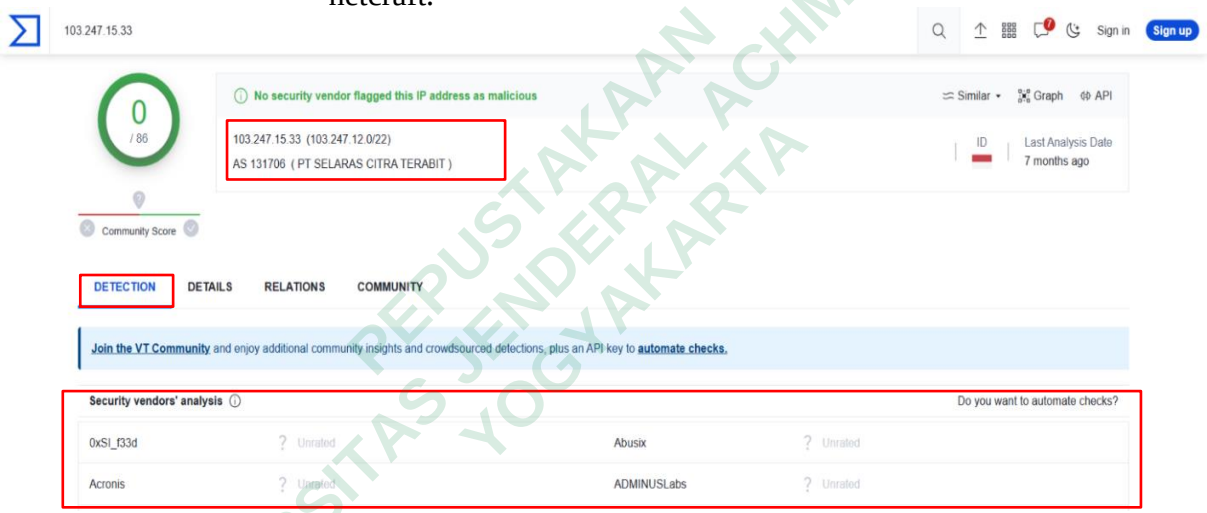
f. Informasi atau data ke lima bagian 7 & 8 mengenai *blog* dan PHP application pada objek penelitian. Terdapat informasi bahwa keseluruhan pada bagian blog dan PHP *application* menggunakan WordPress. Dapat disimpulkan bahwa CMS *(content management system)* pada objek penelitian menggunakan WordPress yang terdevelop dari PHP dn MySql.

g. Informasi ke enam pada bagian 12 mengenai *web browser* targeting pada objek penelitian. Terdapat informasi pada objek penelitian sudah memanfaatkan fungsi spesifik dari *browser* terkhusus dari segi keamanan untuk mengoptimalkan *web application* pada versi *browser* tertentu.

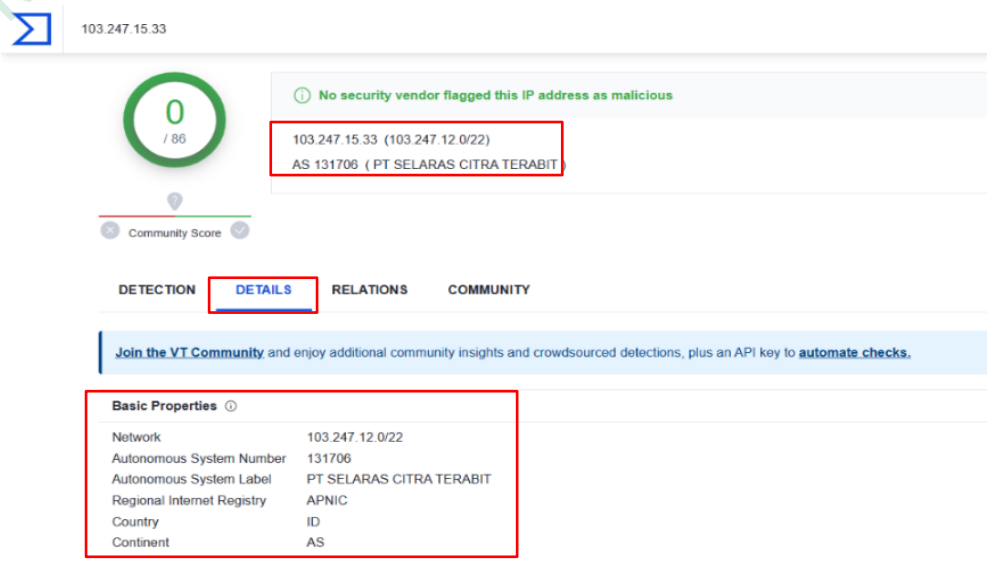
D. Hasil *scanning* virus menggunakan Virus Total

Virus total merupakan layanan atau *tools virus scanning* dan *malware.* Tujuan utamanya adalah menganalisa sebuah file, URL, *Domain*, dan IP *(internet protocol)*. Jika dalam proses analisa dan scanning ditemukan hal yang mencurigakan, Virus Total akan memberikan deteksi secara terperinci. Deteksi tersebut meliputi, *virus*, *worm*, trojan dan berbagai jenis *malware* dengan tujuan untk mendeteksi anacaman pada pengamanan siber. *Report* tersebut seperti yang ditujukan pada Gambar 4.5, Gambar 4.6 dan Gambar 4.7.

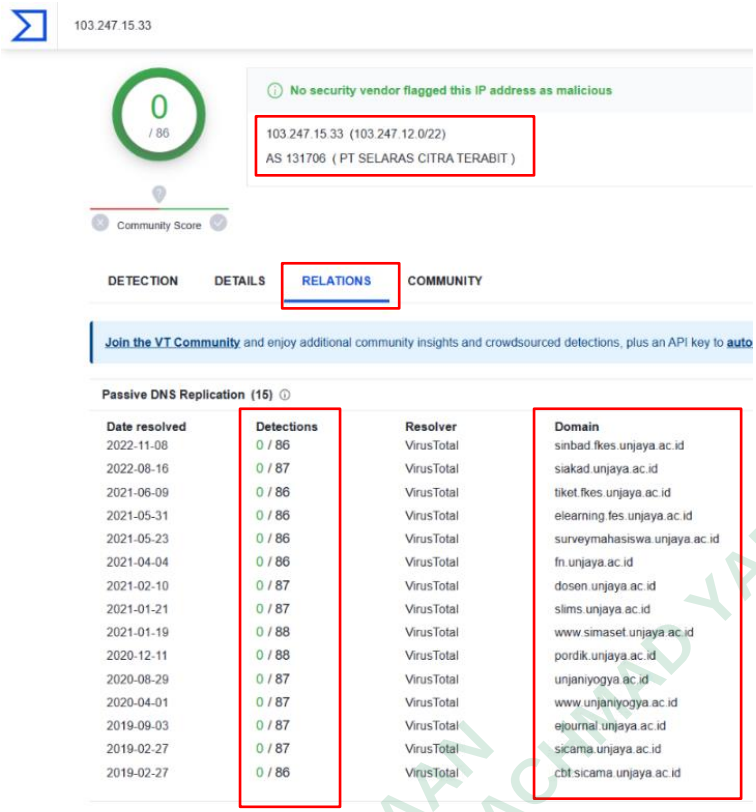
a. Report Virus total menggunakan IP yang terintegrasi dengan netcraft.



Gambar 4.5 Informasi Detection dan Ip Address owner Domain Objek Penelitian Virus Total Tools



Gambar 4.6 Informasi Detail dan Basic Properties PT Selaras Citra Terabit Virus Total Tools



Gambar 4.7 Informasi Relations dan Passive DNS Replication PT Selaras Citra Terabit Virus Total Tools

Berdasarkan hasil *report* dari virus total mengenai alamat IP yang digunakan oleh PT SELARAS CITRA TERABIT yang terintegrasi dengan objek penelitian terdapat 3 hal atau informasi yang didapatkan, yaitu:

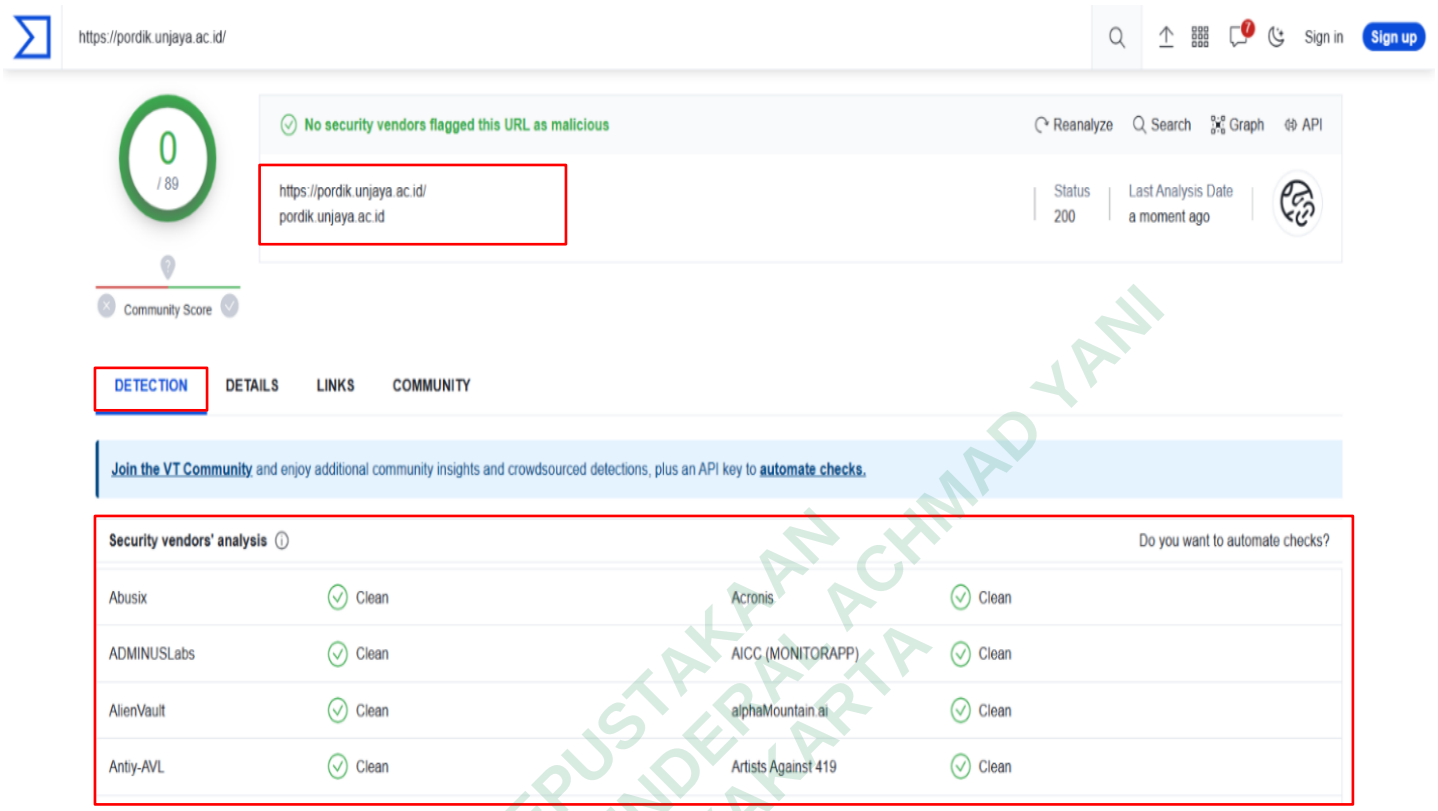
a. Kolom *detection* mengenai analysis keamanan yang dilakukan oleh vendor. Dalam analysis tersebut alamat IP PT SELARAS CITRA TERABIT sudah terkoneksi dengan *vendor* keamanan yang disediakan oleh virus total. Namun, hasil dari *analysis* yang dilakukan oleh vendor tidak memberikan informasi apapun. Hal ini menjadi perlu dianalysis lebih lanjut pada *step* berikutnya.

b. Kolom detail mengenai informasi *basic properties*. Pada informasi tersebut beriskikan *network*, ASN, ASL, *Regional internet Registry.*

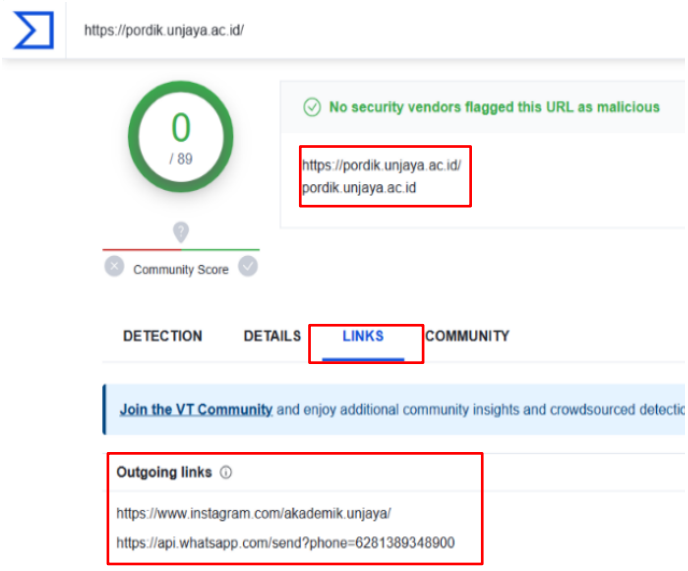
c. Kolom relations mengenai 4 jenis data yang ditemukan. Ke 4 jenis data tersebut diantaranya, *data resolved, detection,*

resolver, domain. Yang perlu dianalysis lebih jauh dari ke 4 jenis data tersebut hanya 2 yang perlu di *highlight.* Yang pertama *detection* dan *domain*. Pada informasi yang ada pada data *detection,* tidak ditemukan adanya informasi resiko keamanan. Hal tersebut direpresntasikan dengan hasil perbandingan 0/86 dari masing masing *data resolved*. Selanjutnya, informasi yang ada pada data domain, memberikan informasi domain – domain apa saja yang terintegrasi dengan alamat IP dari PT SELARAS CITRA TERABIT. Informasi mengenai DNS tersebut bisa menjadi informasi *sensitive* jika ditemukan sebuah *vulnerability* pada fase selanjutnya *yaitu fase reconnaissance* aktif dan *fase exploitation*.

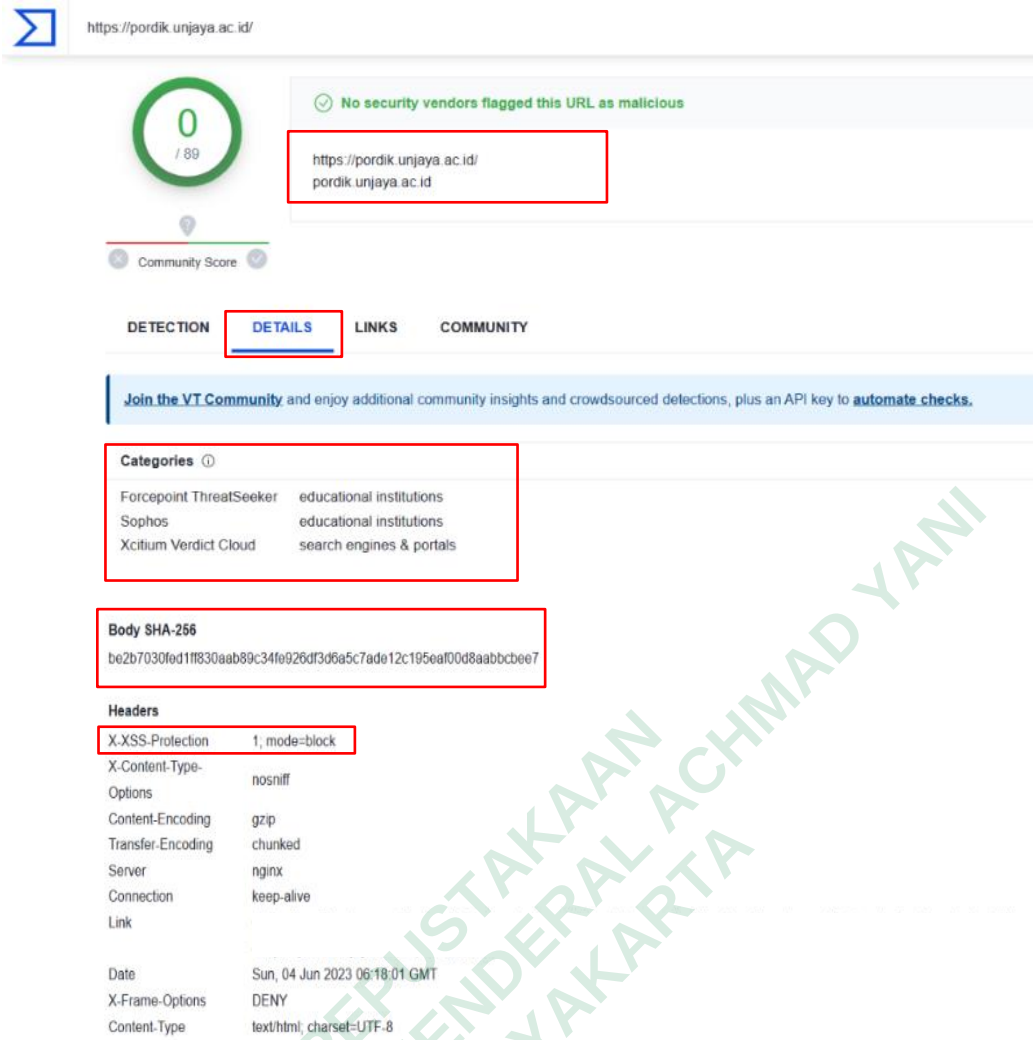
b. Report virus total menggunakan domain objek penelitian



Gambar 4.8 Informasi Detection dan Analysis kemanan Vendor Objek Penelitian Virus Total Tools



Gambar 4. 9 Informasi Link pada Objek Penelitian Virus Total Tools



Gambar 4.10 Informasi Details Categories, Body SHA -256 Public Virus Total Tools

Berdasarkan hasil report yang ditujukan pada Gambar 4.8, Gambar 4. 9 dan Gambar 4.10 dari virus total mengenai DNS pada objek penelitian yang diimplementasikan langsung melalui *website* virus total, ditemukan 3 hal atau informasi yang akan di *analysis.*

a. Kolom detection mengenai detail analysis keamaman yang dilakukan oleh *vendor*. Dalam analysis tersebut DNS objek penelitian sudah terkoneksi dengan beberapa vendor keamanan yang disediakan oleh virus total. Pada informasi tersebut, setiap *vendor* memberikan informasi bahwasannya DNS pada objek penelitian tidak ditemukan suatu hal yang mencurigakan yang dibuktikan dengan hasil *"Clean"* pada setiap vendor

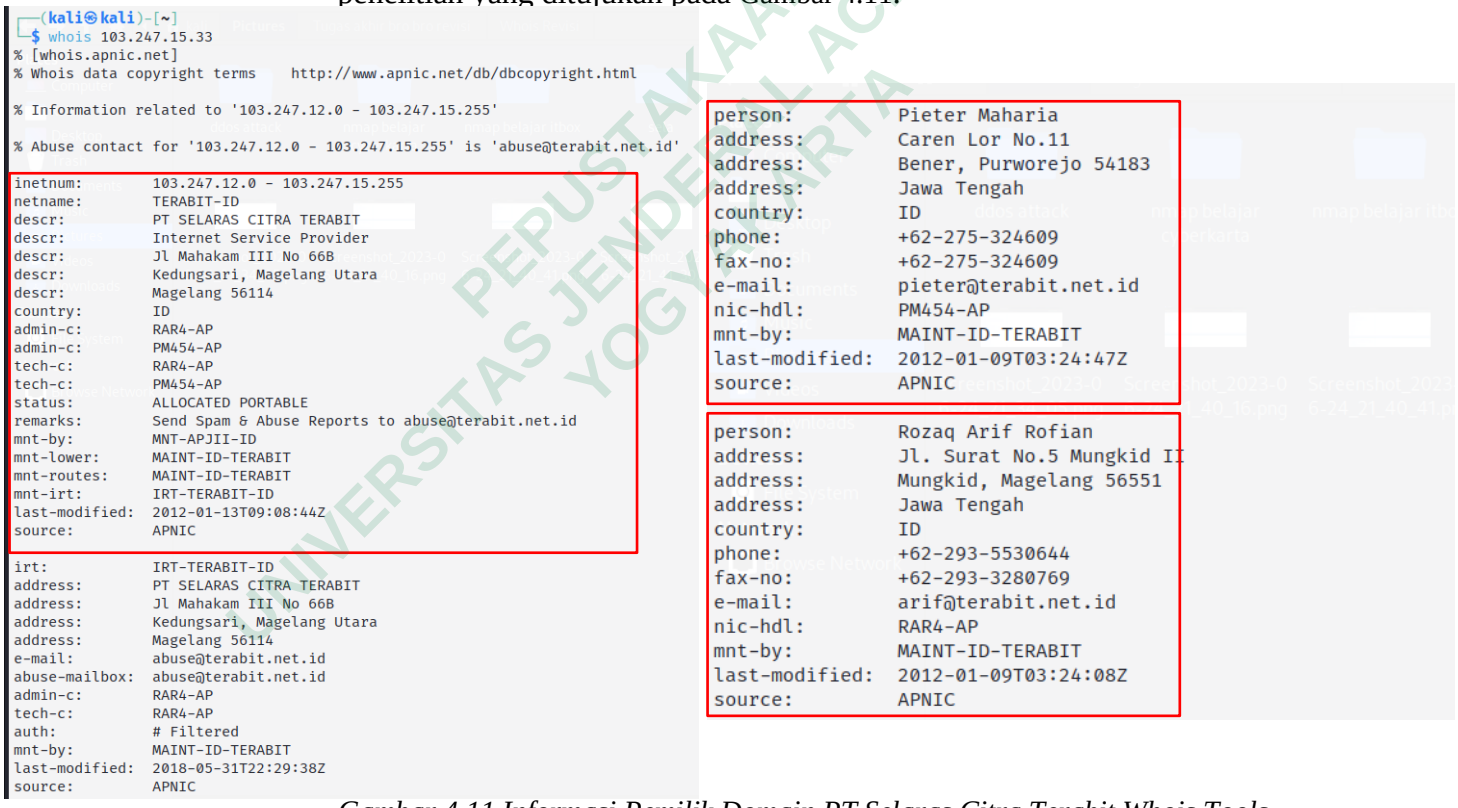
b. Kolom detail menganai informasi detail. Pada kolom informasi detail terdapat 4 data yang ditemukan yaitu, *data categories*, *history*, HTTP *respons*, HTML info. Pada ke 4 data tersebut yang perlu dianalysis lebih jauh yaitu, data categories dan HTTP response. Pada data *categories* terdapat informasi *vendor* keamanan yang sudah menganalisa terhadap objek penelitian yaitu, forcepoint threatseeker, Sophos dan xcitium vidirect cloud. Berdasarkan data yang disampaikan oleh ke 3 vendor tersebut, DNS pada objek penelitian masuk dalam kategori educational institutions dan search engine portals.

c. Kolom detail mengenai HTTP respons. Pada kolom HTTP respons terdapat 6 jenis data yang ditemukan yaitu, final URL, *Serving Ip addres, status code, body length, body SHA 256, heardes.* Pada ke 6 jenis data tersebut yang perlu di *analysis* lebih jauh yaitu ,data body SHA-256. Pada umumnya SHA *(secure high algoritm 256 – bit)* digunakan pada keamanan kriptografi. Kriptogafi sendiri merupakan cara dalam pengamanan informasi dan komunikasi melalui pengkodean khusus. Pengkodean khusus tersebut bisanya dinamakan enkripsi. Fungsi dari enkripsi tersebut untuk meminimalisir dan menghindari dari adanya ancaman keamanan pada suatu layanan dan aplikasi. Keamanan pada suatu layanan dan aplikasi bisanya menggunakan SSL *(secure socket layer).* SSL merupakan sebuah upaya dari layanan dan aplikasi untuk membangun koneksi yang aman (terenkripsi) antara *web server (website)* dengan *client (browser)*. Jadi, dengan adanya informasi body SHA-256 pada layanan objek penelitian bisa disimpulkan dari segi keamanan sudah menerapkan atau menggunakan SSL untuk memininmalisir adanya ancaman pada website.

d. Kolom detail mengenai *headers*. Pada kolom *headers* terdapat informasi X-XSS protection dengan kode 1; mode=block. Berdasarkan informasi tersebut layanan pada objek penelitian sudah menerapkan Anti XSS attack. mode=block untuk mengaktifkan X-Xss protection, jika browser atau situs layanan mendeteksi serangan, hal itu tidak akan merender halaman.

E. Mencari informasi kepemilikan domain menggunakan tools *Whois (who is the owner responsible for a domain name or IP address).*

Pada umumnya whois sendiri memiiliki 2 jenis layanan yaitu whois domain dan whois *privacy*. Berikut penggunaan whois pada objek penelitian yang ditujukan pada Gambar 4.11.



Gambar 4.11 Informasi Pemilik Domain PT Selaras Citra Terabit Whois Tools

Berdasarkan penggunaan tools whois pada IP adress pada objek penelitian ditemukan sebuah informasi sebagai berikut:

a. Inetnum pada objek penelitian ini terbentang pada range IPV4 yaitu, 103.247.12.0 – 103.247.15.255. IPV4 sendiri terdiri dari

3 jenis alamat yaitu, unicast yang mengandalkan mekanisme *point to point* (PTP). Jenis alamat berikutnya *multicast, multicast* bisa menghubungkan jaringan dari pusat ke titik yang lain, dimana titik tersebut masih dalam satu alamat. Jenis alamat yang terakhir yaitu broadcast. *Broadcast* sendiri sistemnya hampir sama seperti *multicast*, yang membedakan skala dari broadcast jauh lebih luas dan besar dengan pendistribusian data relatif singkat, cepat.

b. Netname: dalam net berisikan nama dari range IP adress space. Dalam penelitian ini yang dimaksud adalah TERABIT – ID.
c. Descr : informasi yang disampaikan dalam descr berisi mengenai organisasi yang diakuisisi memiliki *address space*. Dalam penelitian ini yang dimaksud Descr adalah PT SELARAS CITRA TERABIT.
d. Country: informasi yang disampaikan biasanya mengenai 2 huruf kode negara atau ekonomi tempat admin-c berada, yang dituliskan dengan UPPERCASE. Dalam penelitian ini pemilik netname berada di indonesia yang di tuliskan dengan 2 kode yaitu, ID.
e. Admin-c: merupakan person yang memegang NIC (*network information centre handle).* NIC merupakan kunci utama pada objek *"person*". Biasanya pada sebuah instansi memungkinkan memiliki lebih dari 1 role *"person"* object, maka dalam admin-c ini bisa didaftarkan lebih dari 1. Role *"person"* yang ada dalam penelitian ini ada 2: RAR4 – AP dan PM54 – AP.
f. Tech-c : merupakan role person yang memegang dalam NIC. Tech-c sendiri sistemnya sama seperti Admin-c. kontak administratif pada Tech-c harus orang yang seseorang yang secara fisik berada pada bagian jaringan.
g. Mnt-by: merupakan daftar "mntner" terdaftar yang digunakan untuk mengesahkan dan mengautentikasi perubahan. Hal ini

berkaitan dengan hak akses informasi dan database yang dilindungi. Jika ada mntner yang tidak terdaftar dalam list objek Mnt by tidak memiliki hak untuk merubah detail pada *database.* Mntner sendiri merupakan nama unik untuk list objek mnter untuk mengelola dari database. Dalam penelitian ini mnt-by adalah MNT-APJII-ID.

h. Mnt-lower merupakan list objek mnter yang diturunkan oleh mnt-by yang diberikan hak akses untuk mengelola database. Dalam penelitian ini yang dimaksud adalah MAINT-ID-TERABIT.

i. Mnt-routes merupakan hak yang diturunkan atau yang diberikan untuk mengelola objek *"route"*. Dalam penelitian ini Mnt-route adalah MAINT-ID-TERABIT.

j. Mnt-irt dan irt (Incident Respons Team) adalah *database* yang berisi mengenai informasi kontak adminstrator jaringan yang bertanggung jawab untuk menerima laporan ketika ada penyalahgunaan jaringan. Dalam penelitian Mnt-irt dan irt adalah IRT-TERABIT-ID.

k. Source merupakan keterangan dari mana data whois mengenai objek penelitian ditemukan. *Source* pada penelitian ini adalah dari APNIC. APNIC adalah Asian Pacific Network Information Centre.

F. Mencari informasi dan data *sensitive* menggunakan tools google hacking data base dan google dork.

Google hacking data base merupakan kumpulan *query* (permintaan data dari *database*) sekaligus tools untuk mencari sebuah kerentanan, data - data *sensitive* atau informasi pada suatu layanan menggunakan *search engine* seperti google yang berguna bagi seorang penguji *(penetration tester)* untuk melakukan fase dalam *penetration testing*. Google hacking merupakan teknik yang memakai goole dork atau *advance operator the*

google. Dengan menggunakan google dork, seorang penguji (*penetration tester*) dapat melakukan enumerasi pada sistem sesuai dengan yang dibutuhkan. Google dork sendiri memiliki operator, masing masing operator tanggung jawab dan fungsi tersendiri. Dengan memakai operator tersebut seorang penguji (*penetration tester*) bisa mengkhususkan pencarian data lebih rinci lagi. Berikut operator dalam google dork yang ditujukan pada Gambar 4.12.

Google dork cheatsheet

Search filters

Filter	Description	Example
allintext	Searches for occurrences of all the keywords given.	`allintext:"keyword"`
intext	Searches for the occurrences of keywords all at once or one at a time.	`intext:"keyword"`
inurl	Searches for a URL matching one of the keywords.	`inurl:"keyword"`
allinurl	Searches for a URL matching all the keywords in the query.	`allinurl:"keyword"`
intitle	Searches for occurrences of keywords in title all or one.	`intitle:"keyword"`
allintitle	Searches for occurrences of keywords all at a time.	`allintitle:"keyword"`
site	Specifically searches that particular site and lists all the results for that site.	`site:"www.google.com"`
filetype	Searches for a particular filetype mentioned in the query.	`filetype:"pdf"`
link	Searches for external links to pages.	`link:"keyword"`
numrange	Used to locate specific numbers in your searches.	`numrange:321-325`
before/after	Used to search within a particular date range.	`filetype:pdf & (before:2000-01-01 after:2001-01-01)`
allinanchor (and also inanchor)	This shows sites which have the keyterms in links pointing to them, in order of the most links.	`inanchor:rat`
allinpostauthor (and also inpostauthor)	Exclusive to blog search, this one picks out blog posts that are written by specific individuals.	`allinpostauthor:"keyword"`
related	List web pages that are "similar" to a specified web page.	`related:www.google.com`
cache	Shows the version of the web page that Google has in its cache.	`cache:www.google.com`

Gambar 4.12 Enumerasi Cheatsheet Google Dork Tools

Dalam penelitian ini enumerasi yang dilakukan adalah mencari informasi *login* yang ada pada objek penelitian menggunakan operator yang tersedia dalam google dork. Berikut hasil enumarasi *login* pada objek penelitian.

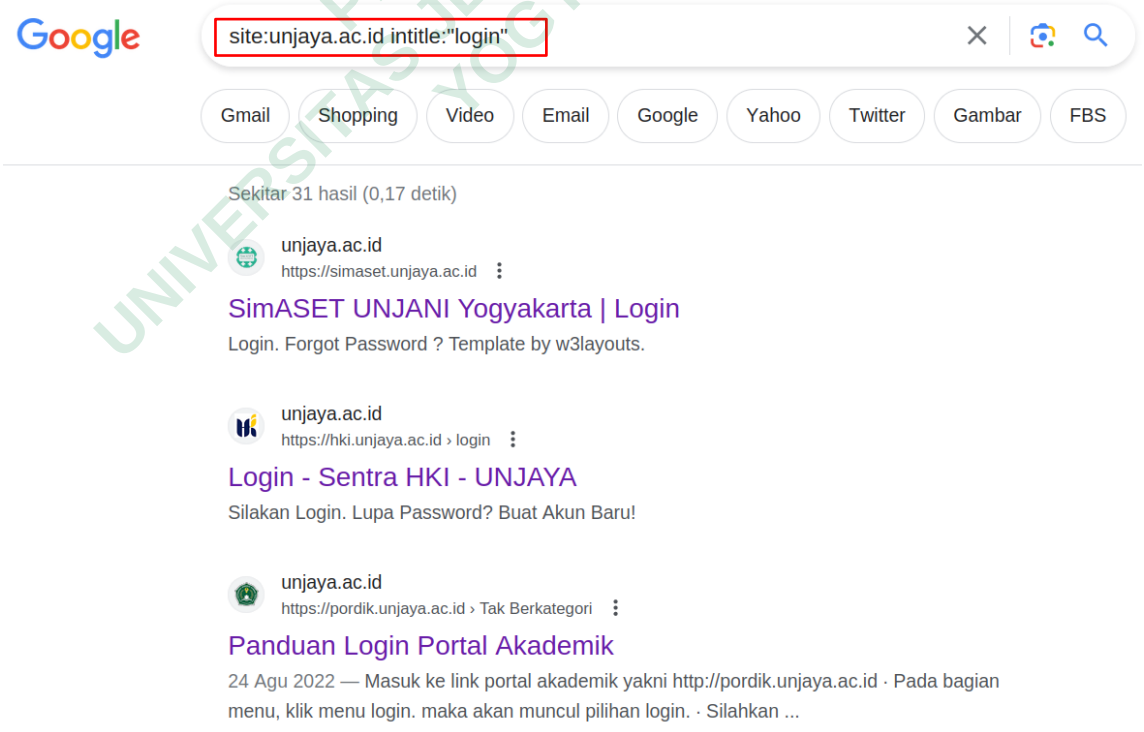
Berikut data *Query* Google dork yang digunakan pada objek penelitian:

Tabel 4.1 Tabel Google Dork List

Google Dork List			
List Query	Search	Result	
		Yes	No
Site	Site:unjaya.ac.id intitle: “login”	✓	
Inurl	“inurl”slot”		✓
Intittle	Pordik unjaya intitle:”index.of”		✓

Berdasarkan *list query* yang ditujukan pada Tabel 4.1 ditemukan pada objek penelitian, terdapat informasi yang ditemukan. Adapun informasi tersebut seperti yang ditujukan pada Gambar 4.13

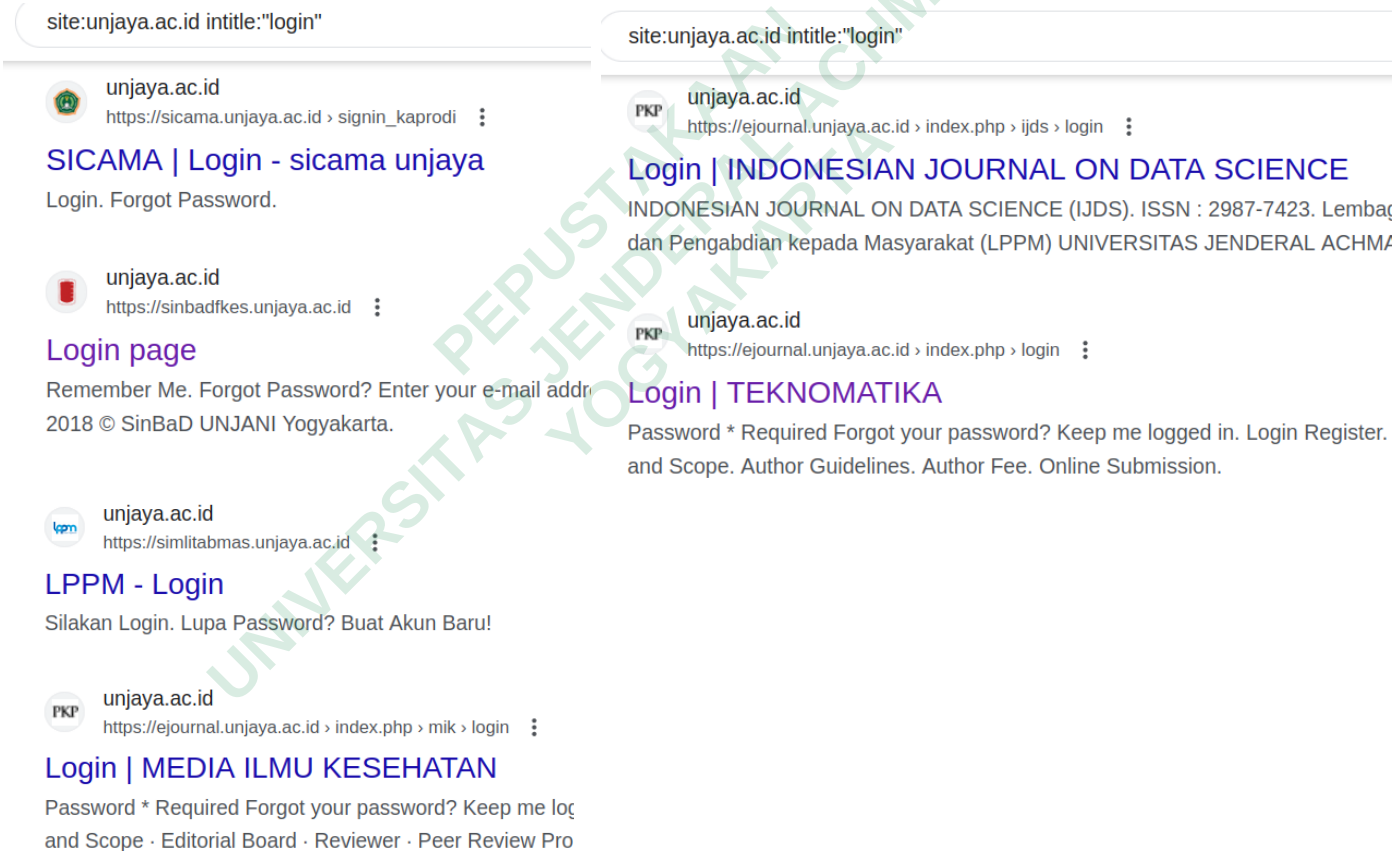
A. Mencari Informasi Login



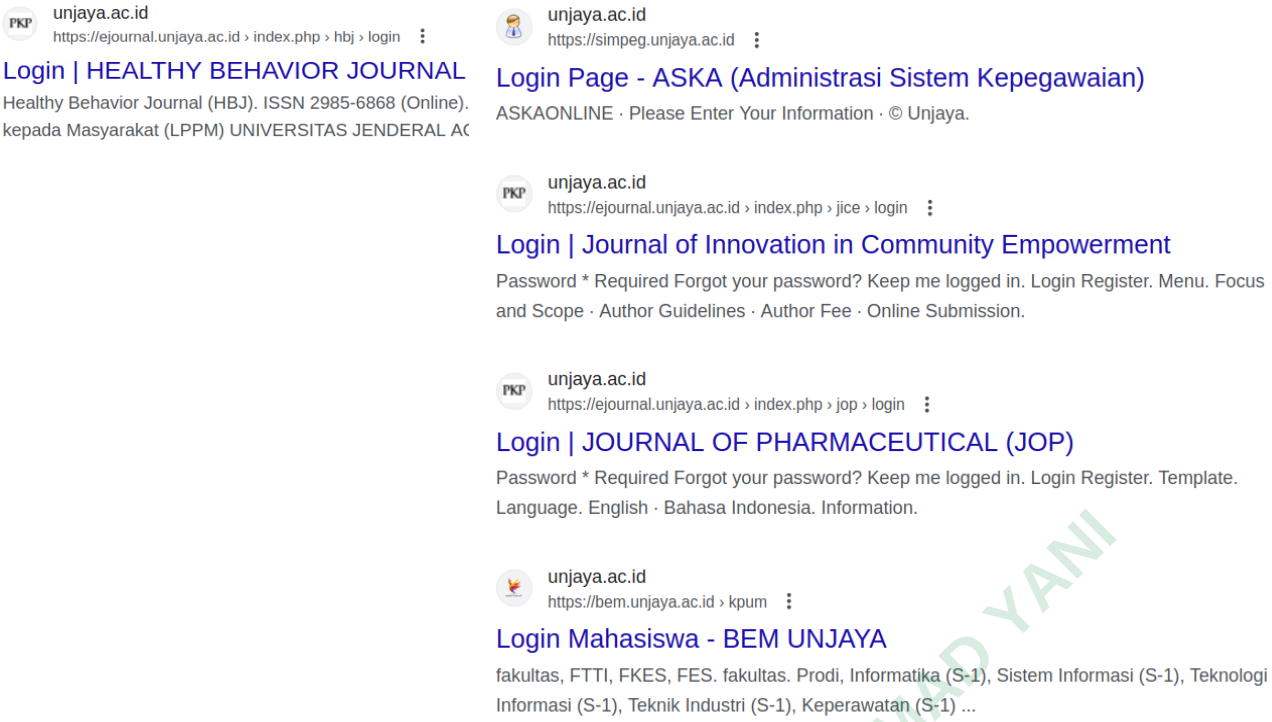
Gambar 4.13 Enumerasia Login pada Objek Penelitian Google Dork Tools

Dalam penggunaan enumerasi dalam mencari informasi login pada objek penelitian, ditemukan sebuah 1 informasi login yaitu, panduan login pada Portal Akademik.

Karena dalam pengumpulan informasi masih kurang, selanjutnya enumerasi dalam mencari informasi login tidak hanya dalam portal akademik, tetapi merambah kedalam situs *web* Universitas Jenderal Achmad Yani Yogyakarta. Berikut hasil tambahan informasi enumerasi dalam mencari informasi login yang ditujukan pada Gambar 4.14 dan Gambar 4.15



Gambar 4.14 Enumerasi Login Pada Layanan Web Unjaya 1



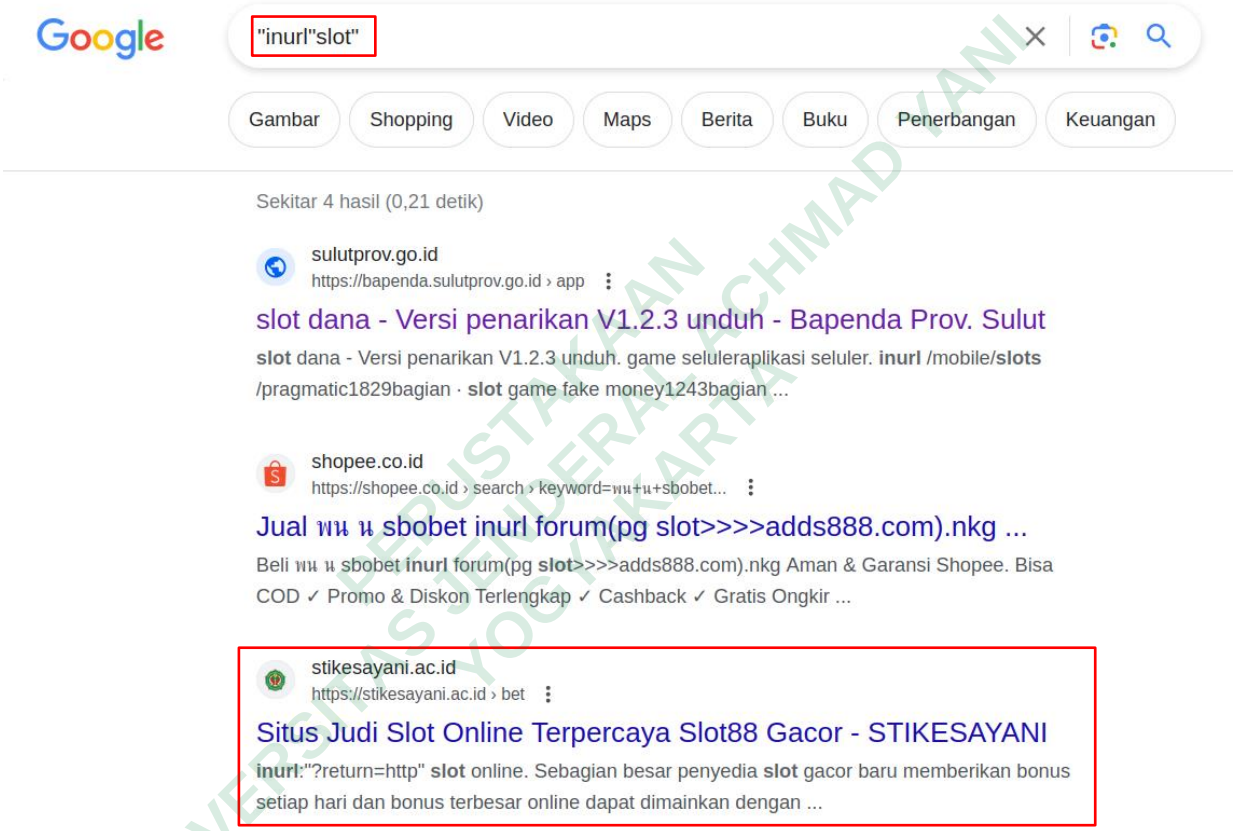
Gambar 4.15 Enumerasi Login Pada Layanan Web Unjaya 2

Dalam penggunaan enumerasi dalam informasi tambahan mencari sistem login situs *web* Universitas Jenderal Achmad Yani Yogyakarta, ditemukan sebuah 15 informasi login yaitu, login sentra HKI- Unjaya, panduan login Portal Akademik, SICAMA login, LPPM login, login | TEKNOMATIKA, login |HEALTHY BEHAVIOR JOURNAL, login | INDONESIA JOURNAL ON DATA SCIENCE, simASET unjani Yogyakarta| login, login, login| Journal of innovation in comunnity empowerment, login page–ASKA (adminitrasi keuangan kepegawaian), login| ilmu media kesehatan, login mahasiswa – BEM unjaya, login| Bowl of Hygeia Journal.

Google hacking database tersendiri merupakan *repository* (archiving atau tempat untuk menyimpan) yang dimana berisikan google dork yang bisa dipakai mencari beberapa kategori yang dibutuhkan. Goole dork juga membantu dalam penyeledikan dalam mencari sebuah kerentanan untuk meningkatkan efisiensi pada fase *intellegence gathering* menggunakan teknik OSINT (*Open Source Intellegence*).

B. Mencari Informasi Black Hat SEO “Slot”

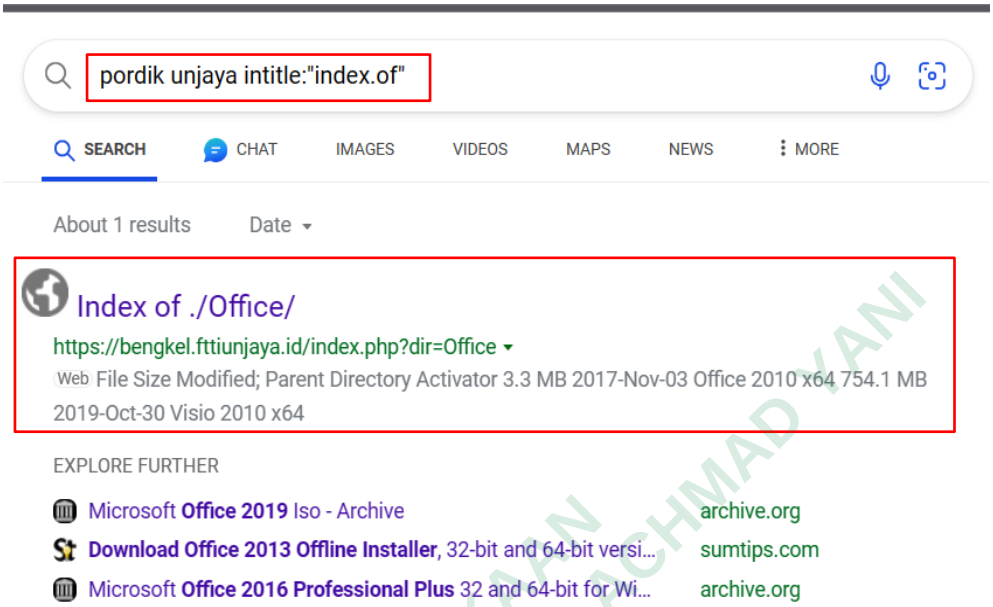
Black hat seo merupakan *tools* untuk meningkatkan optimasi *serach engine* sebuah situs web dengan melanggar *tearm of service* (Bello & Otobo, 2018). Berikut hasil dari *query* mencari informasi black hat seperti pada Gambar 4.16



Gambar 4.16 Informasi Black hat SEO Google Dork Tools

Berdasarkan data tersebut, tidak ditemukan sebuah black hat SEO pada objek penelitian. Namun informasi lain yang ditemukan terdapat black hat SEO pada Stikes Universitas Jenderal Achmad Yani Cimahi dan temuan ini tidak termasuk dalam scope penelitian. seperti yang ditujukan pada Gambar 4.16.

C. Menemukan repositori layanan menggunakan index of



Gambar 4.17 Informasi Index.of Pada Objek Penelitian 1

Gambar 4.18 Informasi Index.of Pada Objek Penelitian 2

Berdasarkan data tersebut ditemukan sebuah *repository* dari salah satu layanan pada Universitas Jenderal Achmad Yani Yogyakarta yaitu bengkel FTTI yang ter index.of dan repositiry tersebut tidak masuk kedalam scope penelitian atau pengujian. seperti yang ditujukan pada Gambar 4.17 dan Gambar 4.18

4.2.2.2 Active reconnaisssance

Active reconnaissance merupakan pengumpulan informasi dan data mengenai objek, layanan atau target yang akan diteliti secara langsung berinteraki dengan objek, layanan atau target yang akan diteliti. Pada tahap *active reconnaissance* informasi yang didapatkan bersifat *real* dan terupdate. Untuk mendapatkan informasi dan data tersebut pada *active reconnaissance* menggunakan *port scanning* dan *vulnerability scannn*

ing melalui terminal atau kernel Kali Linux. Tujuan dilakukan *active reconnaissance* adalah untuk mengumpulkan informasi sebanyak mungkin dan bisa mengidentifikasi kemungkinan adanya sebuah kerentanan yang didapatkan.

A. Mengeksplorasi keamanan jaringan menggunakan *tools* Nmap

```
└─$ sudo nmap pordik.unjaya.ac.id
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-25 19:08 EDT
Nmap scan report for pordik.unjaya.ac.id (103.247.15.33)
Host is up (0.019s latency).
rDNS record for 103.247.15.33: ip-33-15-247.terabit.net.id
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 5.30 seconds
```

Gambar 4.19 Informasi Port Terbuka pada Objek Penelitian Nmap Tools

```
└─$ nmap -T4 -A  pordik.unjaya.ac.id
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-25 19:10 EDT
Nmap scan report for pordik.unjaya.ac.id (103.247.15.33)
Host is up (0.055s latency).
rDNS record for 103.247.15.33: ip-33-15-247.terabit.net.id
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE          VERSION
80/tcp   open  http             nginx
|_http-title: Did not follow redirect to https://pordik.unjaya.ac.id/
443/tcp  open  ssl/http         nginx
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=*.unjaya.ac.id
| Subject Alternative Name: DNS:*.unjaya.ac.id, DNS:unjaya.ac.id
| Not valid before: 2022-12-19T07:53:46
|_Not valid after:  2024-01-20T07:53:45
|_ssl-date: TLS randomness does not represent time
8081/tcp open  blackice-icecap?
| fingerprint-strings:
|   HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 13
|_    Found
```

Gambar 4.20 memeriksa sistem operasi dan versi, pemeriksaan skrip Pada Objek Penelitian Nmap Tools

```
└─$ nmap pordik.unjaya.ac.id -sV -T5 -p 80 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-25 19:17 EDT
Nmap scan report for pordik.unjaya.ac.id (103.247.15.33)
Host is up (0.054s latency).
rDNS record for 103.247.15.33: ip-33-15-247.terabit.net.id

PORT   STATE SERVICE VERSION
80/tcp open  http    nginx
|_http-title: Did not follow redirect to https://pordik.unjaya.ac.id/

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.13 seconds
```

Gambar 4.21 Hasil Vulnerability Scanner Pada Port 80 Objek Penelitian Nmap Tools

```
└─$ nmap pordik.unjaya.ac.id -sV -T5 -p 443 -A
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-25 19:18 EDT
Nmap scan report for pordik.unjaya.ac.id (103.247.15.33)
Host is up (0.19s latency).
rDNS record for 103.247.15.33: ip-33-15-247.terabit.net.id

PORT    STATE SERVICE  VERSION
443/tcp open  ssl/http nginx
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.unjaya.ac.id
| Subject Alternative Name: DNS:*.unjaya.ac.id, DNS:unjaya.ac.id
| Not valid before: 2022-12-19T07:53:46
|_Not valid after:  2024-01-20T07:53:45
|_http-title: PORTAL AKADEMIK &#8211; Universitas Jenderal Achmad Yani Yogya...
|_http-generator: WordPress 6.0.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.38 seconds
```

Gambar 4.22 Hasil Vulnerability Scanner Pada Port 443 Objek Penelitian Nmap Tools

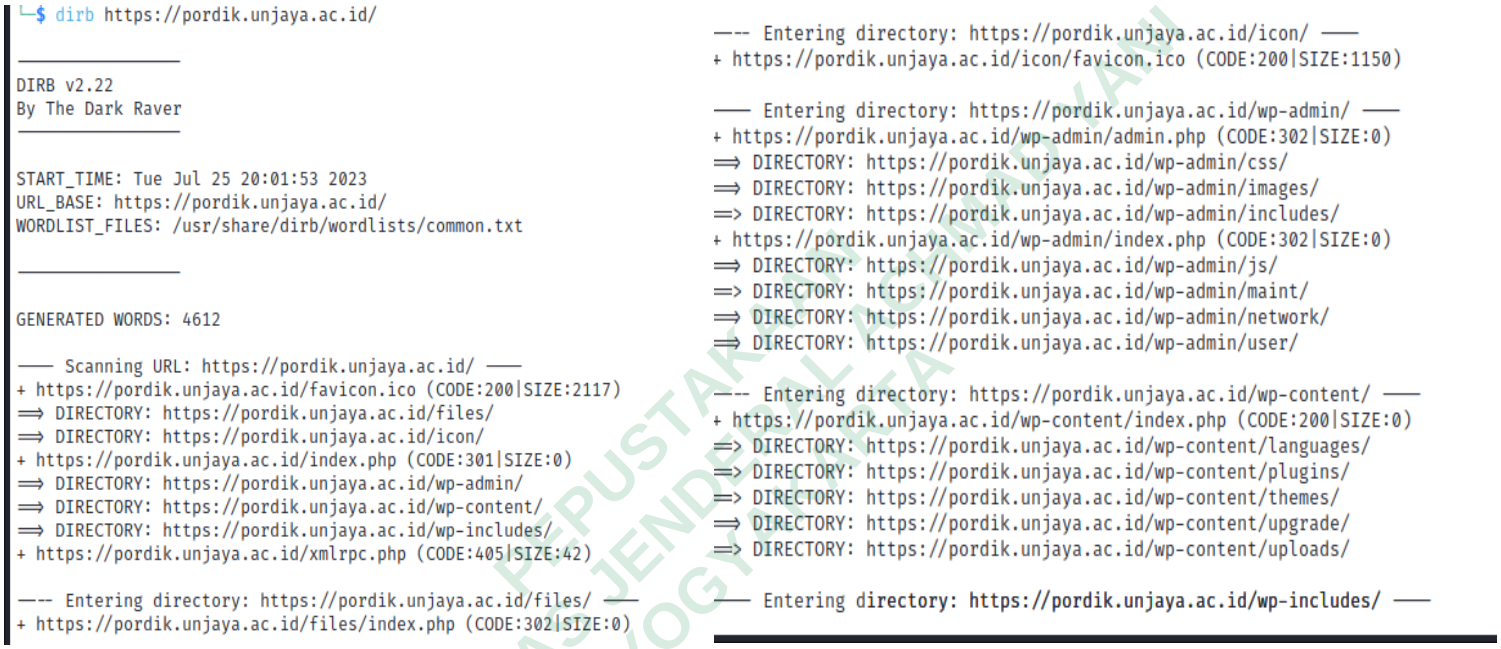
```
└─$ sudo nmap -sU -T4 -sV pordik.unjaya.ac.id -p 53
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-25 19:20 EDT
Stats: 0:00:33 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Stats: 0:01:18 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for pordik.unjaya.ac.id (103.247.15.33)
Host is up (0.0016s latency).
rDNS record for 103.247.15.33: ip-33-15-247.terabit.net.id

PORT   STATE         SERVICE VERSION
53/udp open|filtered domain

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 99.35 seconds
```

Gambar 4.23 Hasil Vulnerability Scanner Pada Port 53 Objek Penelitian Nmap Tools

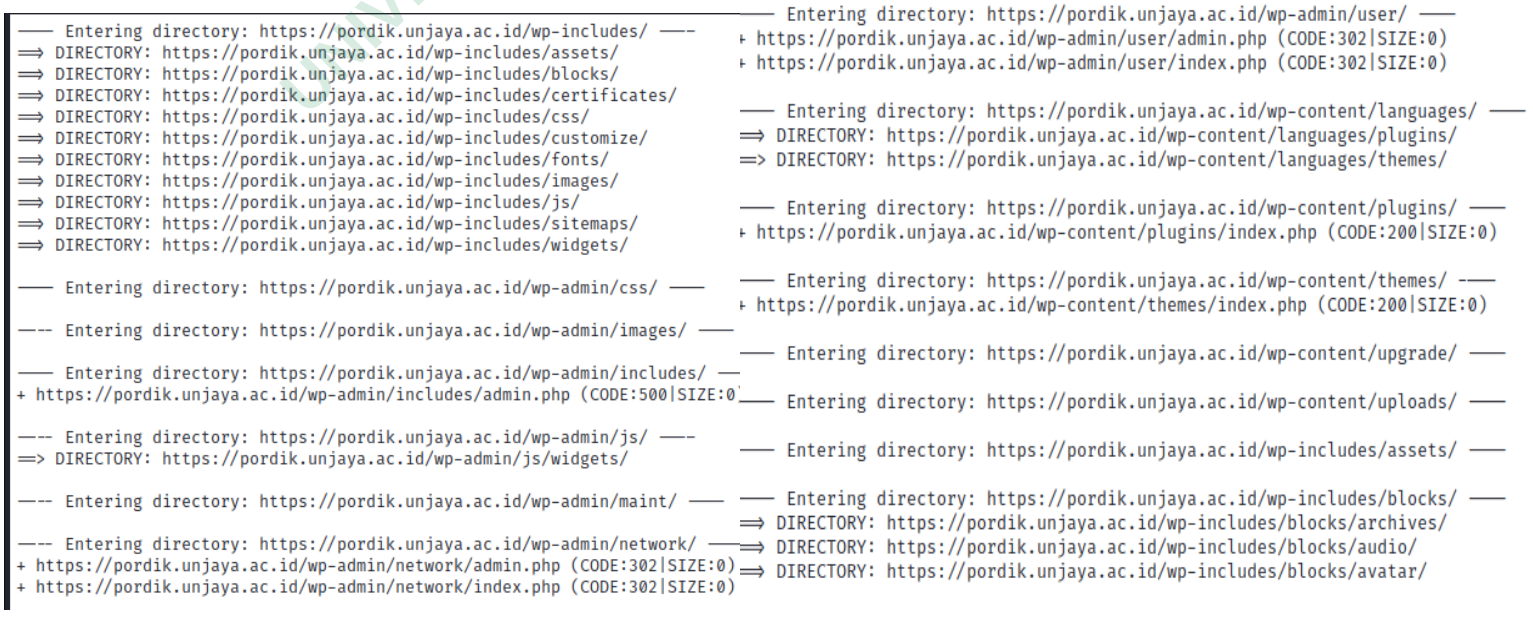
a. Berdasarkan penggunaan *tools* nmap yang dilakukan pada objek penelitian terdapat rincian informasi mengenai *port*. *Port* yang terbuka pada objek penelitian ada 3 yaitu, port 80, 443, 8081 dengan informasi yang disampaikan pada data dan *service* seperti yang ditujukan pada Gambar 4.19
b. Penggunaan *vulnerability scanning* pada masing-masing *port,* juga memberikan sebuah informasi sebagai berikut dan juga ditujukan pada,Gambar 4.20 Gambar 4.21Gambar 4.22:
    - Data port 80 dalam keadaan terbuka dan *service* yang digunakan pada *port* tersebut adalah http
    - Data port 443 dalam keadaan terbuka dan *service* yang digunakan pada port tersebut ssl
    - Data port 8081dalam keadaan terbuka dan service yang digunakan pada port tersebut blackice-icecap
c. Penggunaan *vulnerability scanning* untuk mengetahui pada DNS dengan menggunakan perintah sU merupakan protokol UDP dan spesifikasi port. Port yang digunakan untuk DNS adalah 53. Informai yang ditemuka sebagai berikut dan juga ditujukan padaGambar 4.23:
    - Data port 53 dalam keadaan terbuka dan *service* yang digunakan pada *port* tersebut adalah domain.

B. Mencari direktori dan *file sensitive* menggunakan *tools* dirbuster

Dirbuster merupakan *tools reconnaisance* aktif untuk layanan *web*. Dengan menggunakan dirbuster seorang penguji (*penetration tester*) bisa melihat sebuah *hidden directory* atau *hidden website* didalam sebuah domain. Berikut hasil penggunaan *tools* yang dilakukan oleh dirbuster seperti pada Gambar 4.24, Gambar 4.25 dan Gambar 4.26



Gambar 4.24 List Hidden Directory Pada Objek Penelitian 1 Dirb Tools



Gambar 4.25 List Hidden Directory Pada Objek Penelitian 2 Dirb Tools

```
---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/images/ ----
==> DIRECTORY: https://pordik.unjaya.ac.id/wp-includes/images/media/
==> DIRECTORY: https://pordik.unjaya.ac.id/wp-includes/images/smilies/

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/js/ ----
==> DIRECTORY: https://pordik.unjaya.ac.id/wp-includes/js/dist/
==> DIRECTORY: https://pordik.unjaya.ac.id/wp-includes/js/jquery/
+ https://pordik.unjaya.ac.id/wp-includes/js/swfobject.js (CODE:200|SIZE:10231)
==> DIRECTORY: https://pordik.unjaya.ac.id/wp-includes/js/thickbox/
==> DIRECTORY: https://pordik.unjaya.ac.id/wp-includes/js/tinymce/

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/sitemaps/ ----
==> DIRECTORY: https://pordik.unjaya.ac.id/wp-includes/sitemaps/providers/

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/widgets/ -----

---- Entering directory: https://pordik.unjaya.ac.id/wp-admin/js/widgets/ ----

---- Entering directory: https://pordik.unjaya.ac.id/wp-content/languages/plugins/ ----

---- Entering directory: https://pordik.unjaya.ac.id/wp-content/languages/themes/ ----

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/blocks/archives/ ----

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/blocks/audio/ ----

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/blocks/avatar/ ----

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/blocks/block/ ----

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/blocks/button/ ----

---- Entering directory: https://pordik.unjaya.ac.id/wp-includes/blocks/buttons/ ----
```

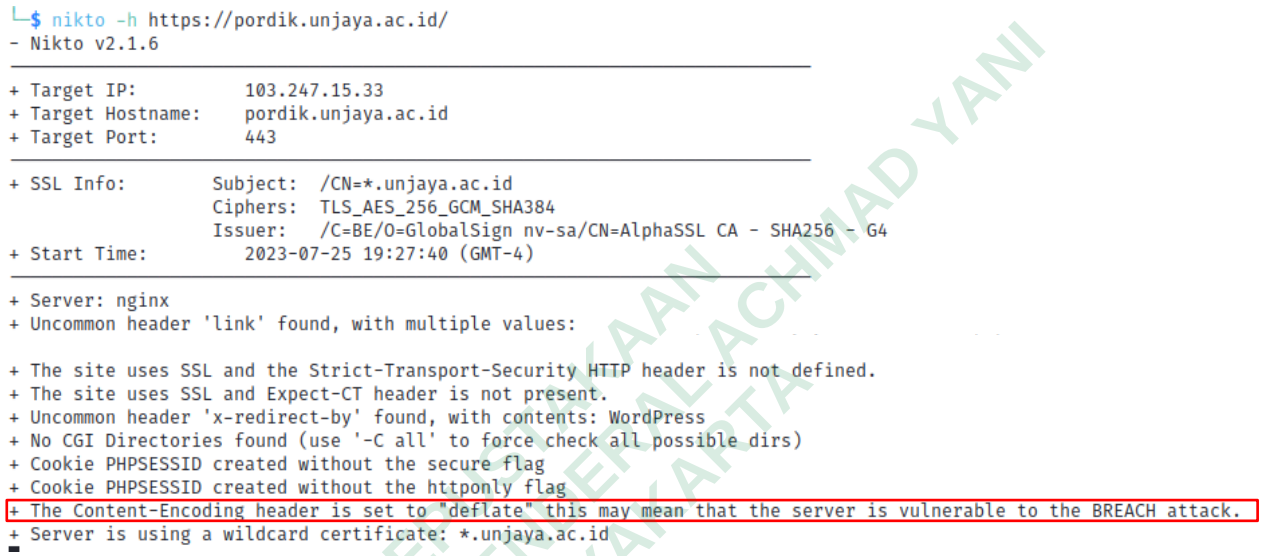
Gambar 4.26 List Hidden Directory Pada Objek Penelitian 3 Dirb Tools

Berdasarkan penggunaa *tools* dirbuster yang dilakukan ke objek penelitian, terdapat sebuah informasi mengenai *hidden directory* yang ditemukan.Sebelum keluar hasil total dari *hidden dirctory* yang ditemukan, dalam prosesnya dirbuster akan mengeluarkan l*ist directory* dan masing masing status codenya. Berikut penjelasan hasil yang ditemukan oleh dirbuster.

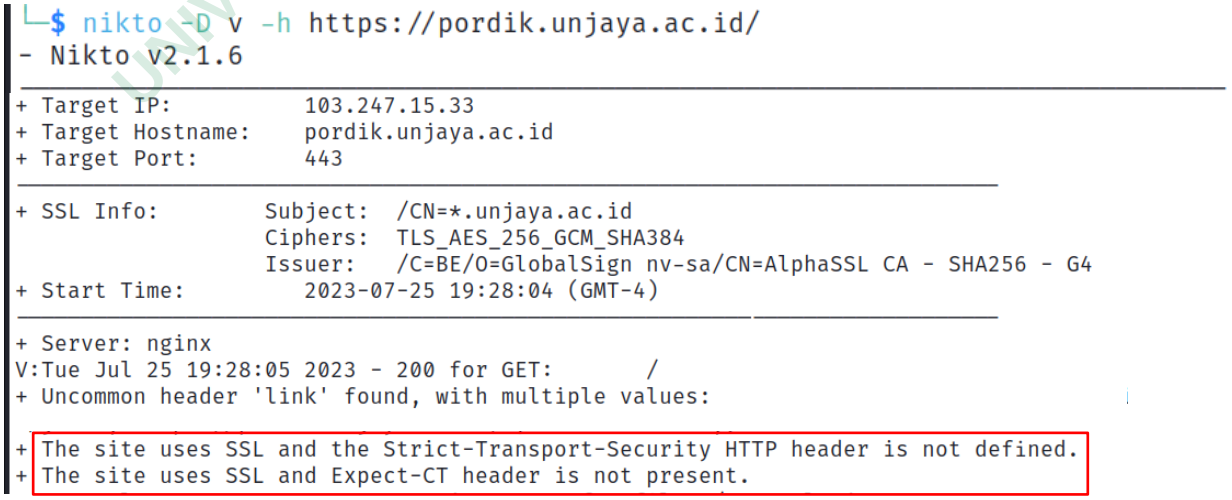
a. Dalam dirbuster terdapat *list directory* yang bercirikan dengan tanda (+) dan *code*. *List directory* dengan *status code* 200 berjumlah 5, *List directory* dengan *status code* 301 berjumlah 1, *List directory* dengan status code 302 berjumlah 7, *List directory* dengan *status code* 405 berjumlah 1, *List directory* dengan *status code* 500 berjumlah 3.
b. *Hidden directory* yang ditemukan dirbuster berjumlah 91 *hidden directory*. Masing-masing *hidden directory* tersebut berada dalam *list directory* yang ditemukan.

C. *Vulnerability scanning* menggunakan Nikto

Nikto merupakan *tools* yang dibuat dengan bahasa pemrograman Perl. Nikto merupakan tools untuk pemindaian kerentanan khusus untuk *web server* (Indyawan, 2022). Berikut hasil *scanning* seperti yang ditujukan pada Gambar 4.27, Gambar 4.28Gambar 4.29Gambar 4.30, Gambar 4.31 dan Gambar 4.32.



Gambar 4.27 Menemukan Vulnerable Breach Attack Pada Content Encoding Header Objek Penelitian Nikto Tools



Gambar 4.28 Melihat Proses Debugging Pada Objek Penelitian Nikto Tools

```
└─$ nikto -Tuning 9 -h pordik.unjaya.ac.id
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          103.247.15.33
+ Target Hostname:    pordik.unjaya.ac.id
+ Target Port:        80
+ Start Time:         2023-07-25 19:29:25 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agen
+ The X-Content-Type-Options header is not set. This could allow the user agent to
+ Root page / redirects to: https://pordik.unjaya.ac.id/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 680 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2023-07-25 19:30:04 (GMT-4) (39 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

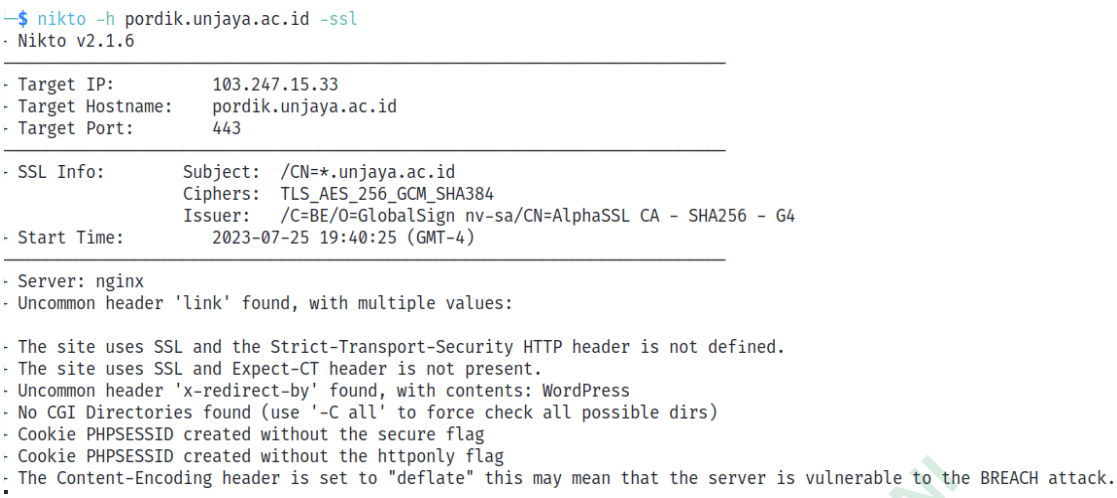
Gambar 4.29 Melihat Kerentanan SQL Injection Attack Pada Port 80 Nikto Tools

```
└─$ nikto -Tuning 4 -h pordik.unjaya.ac.id
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          103.247.15.33
+ Target Hostname:    pordik.unjaya.ac.id
+ Target Port:        80
+ Start Time:         2023-07-25 19:30:52 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the us
+ The X-Content-Type-Options header is not set. This could allow the user ag
+ Root page / redirects to: https://pordik.unjaya.ac.id/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 935 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2023-07-25 19:31:51 (GMT-4) (59 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Gambar 4.30 Melihat Kerentanan Injection Attack Pada Port 80 Nikto Tools

```
└─$ nikto -Tuning 69 -h pordik.unjaya.ac.id
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          103.247.15.33
+ Target Hostname:    pordik.unjaya.ac.id
+ Target Port:        80
+ Start Time:         2023-07-25 19:33:37 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user ag
+ The X-Content-Type-Options header is not set. This could allow the user agent t
+ Root page / redirects to: https://pordik.unjaya.ac.id/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 563 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2023-07-25 19:34:13 (GMT-4) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Gambar 4.31 Melihat Kerentanan Denial of Services , SQL Injection Attack Pada Port 80 Nikto Tools



Gambar 4.32 Vulnerable Scanner Pada Port 443

Berdasarkan penggunaan *tools* Nikto yang dilakukan pada objek penelitian terdapat informasi sebagai berikut:

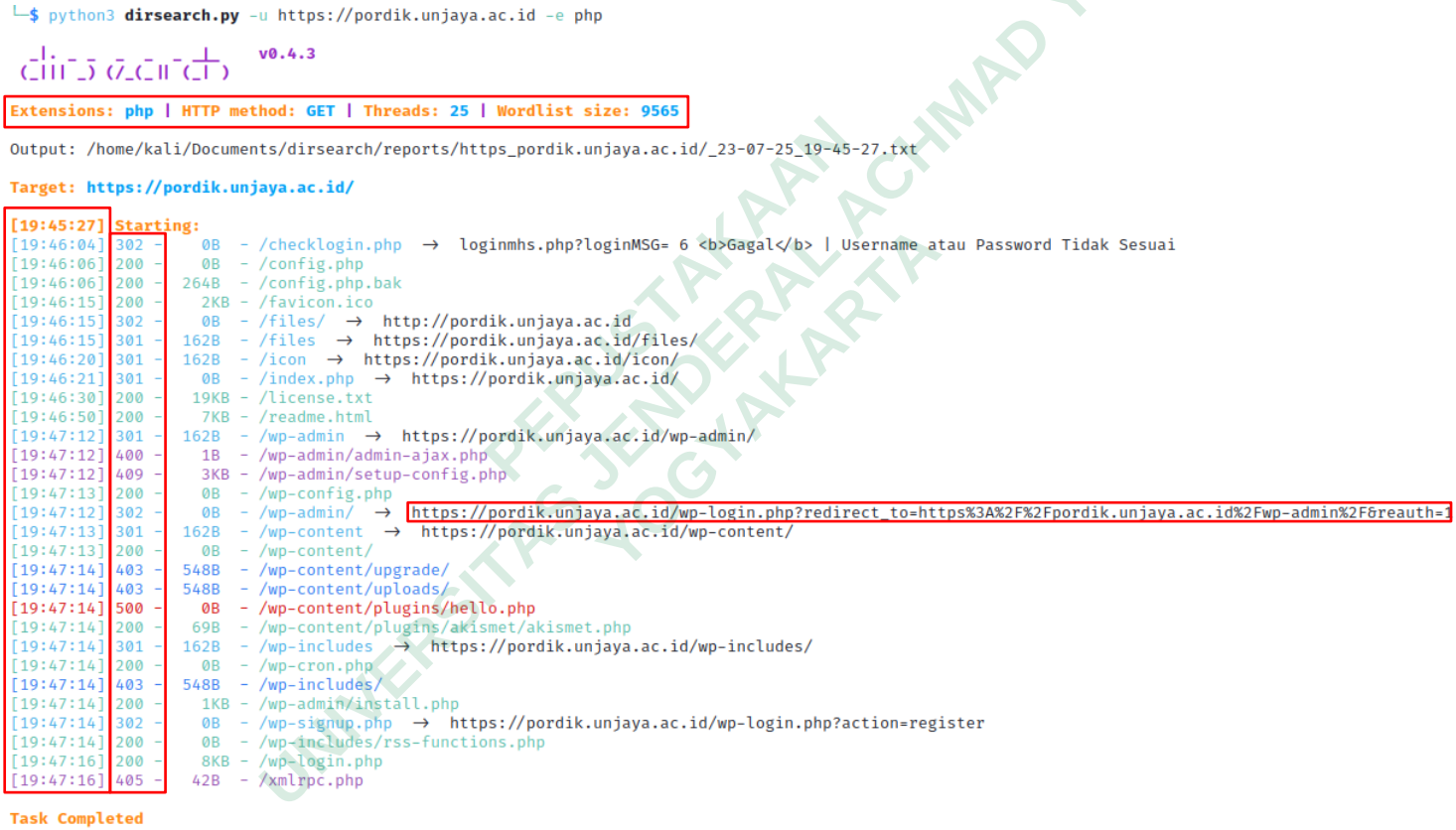
a. Dalam *server* tedapat sebuah *vulnerable* yaitu, kemungkinan server bisa diserang dan mengindeksi *breach attack* seperti yang ditunjukan pada Gambar 4.27
b. Pada proses vulnerability scanner menemukan debugging pada sistem yang diterlatak pada port 443 seperti yang ditunjukan pada Gambar 4.28
c. Pada port 80 yang sudah ditunningkan untuk pemindaian celah pada SQL Injection, injection, DDos dan SQL terdapat 3 informasi yang ditemukan:
    - Anti clickjacking x-frame option header tidak ditampilkan seperti yang ditunjukan pada Gambar 4.29
    - The XSS protection header is not defined. This header can hint to the user agent to protect against some forms of XSS. Header perlindungan x XSS tidak ditentukan. Header ini dapat memberi petunjuk kepada agen pengguna untuk melindungi dari beberapa bentuk seranngann XSS. Hal ini penting untuk melindungi dari serangan XSS . Disisi lain hal ini juga memungkinkan objek penelitian bisa diterkena serangan dari celah SQL

Injection dan XSS (*Cross Site Scripting*) seperti yang ditunjukan pada Gambar 4.30.

- Ditemukan informasi megenai celah serangan jenis DDos Attack dan SQL Injection seperti yang ditunjukan pada Gambar 4.31
- Pada port 433 ditemukan informasi site uses SSL and the Strict – Transport – Security HTTP yang ditunjukan pada Gambar 4.32

D. Memaksimalkan mencari *hidden directory* menggunakan *tools dirsearch.*

Dirsearch merupakan tools yang di *develop* menggunakan bahasa pemrograman *python* untyuk melihat, menemukan *hidden dirctory* dan *hidden web.* Dirsearch sendiri bekerja dengan *multithreading* yang artinya memungkinkan beberapa tugas dapat dilakukan dalam 1 proses. Berikut hasil penggunaan *tools* dirsearch yang dilakukan pada objek penelitian, seperti yang ditujuka pada Gambar 4.33.



Gambar 4.33 Menemukan Informasi Sensitive Wp-admin Objek Penelitian Dirsearch Tools

Berdasarkan hasil report yang disampaikan oleh dirsearch menampilkan informasi yang terbagi menjadi 3 kolom. Kolom 1 mengenai waktu, kolom ke 2 tentang status, kolom ke 3 berisikan informasi penting yang perlu dianalisa. Pada header dirsearch terdapat informasi mengenai *Extensions* yang digunakan menggunakan PHP, HTTP method dengan

GET yang artinya mengambil data dari *server*, *Threads* (benang) sebanyak 25, *Wordlist size* sejumlah 9565. Berbeda dengan hasil yang dikeluarkan oleh dirbuster, dirsearch lebih mudah dibaca dan dipahami.

E. Menganalisa *hidden directory* menggunakan tools dirhunt

Dirhunt memiliki fungsionalitas yang sama seperti dirbuster dan dirsearch. Teknik yang digunakan oleh dirsearch adalah *crawling*. Berikut hasil dari penggunaan *tools* dirhunt pada objek penelitian, seperti ditujukan pada Gambar 4.34, Gambar 4.35, Gambar 4.36.

Gambar 4.34 Analisa Hidden Directory Objek Penelitian 1 Dirhunt Tools

```
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/isikrs.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/isikrs_nr.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/isikrs_nr.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/konfirmasi.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/konfirmasi.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/krs.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/krs.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/logout.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/logout.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/password.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/password.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/plugins/upload/delete.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/plugins/upload/delete.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/plugins/upload/download.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/plugins/upload/download.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/plugins/upload/upload.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/plugins/upload/upload.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/rekapkeu.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/rekapkeu.php
[301] http://pordik.unjaya.ac.id:80/mahasiswa/transkrip.php  (Redirect)
    Redirect to: https://pordik.unjaya.ac.id/mahasiswa/transkrip.php
```

Gambar 4.35 Analisa Hidden Directory Objek Penelitian 2 Dirhunt Tools

```
[403] https://pordik.unjaya.ac.id/orangtua/bootstrap/js/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/dist/img/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/font-awesome/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/dist/css/skins/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/plugins/jQuery/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/bootstrap/fonts/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/font-awesome/fonts/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/ionicons/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/ionicons/fonts/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/plugins/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/plugins/fastclick/  (Generic)
[403] https://pordik.unjaya.ac.id/orangtua/plugins/slimScroll/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/bootstrap/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/bootstrap/js/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/dist/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/fastclick/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/dist/css/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/jQuery/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/bootstrap/css/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/morris/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/jvectormap/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/daterangepicker/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/bootstrap-wysihtml5/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/dist/js/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/datatables/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/dist/css/skins/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/iCheck/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/iCheck/flat/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/slimScroll/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/sparkline/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/common/js/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/datepicker/  (Generic)
[403] https://pordik.unjaya.ac.id/mahasiswa/plugins/knob/  (Generic)
[404] https://pordik.unjaya.ac.id/orangtua/plugins/jQuery/text/  (Not Found)
[404] https://pordik.unjaya.ac.id/orangtua/plugins/jQuery/application/  (Not Found)
[403] https://pordik.unjaya.ac.id/mahasiswa/dist/img/  (Generic)
[404] https://pordik.unjaya.ac.id/mahasiswa/plugins/jQuery/text/  (Not Found)
[404] https://pordik.unjaya.ac.id/mahasiswa/plugins/jQuery/application/  (Not Found)
[403] https://pordik.unjaya.ac.id/mahasiswa/bootstrap/fonts/  (Generic)
[404] https://pordik.unjaya.ac.id/mahasiswa/plugins/sparkline/text/  (Not Found)
[404] https://pordik.unjaya.ac.id/mahasiswa/plugins/datepicker/mm/  (Not Found)
[404] https://pordik.unjaya.ac.id/mahasiswa/plugins/datepicker/mm/dd/  (Not Found)
[404] https://pordik.unjaya.ac.id/mahasiswa/plugins/daterangepicker/MM/  (Not Found)
[404] https://pordik.unjaya.ac.id/mahasiswa/plugins/daterangepicker/MM/DD/  (Not Found)
[404] https://pordik.unjaya.ac.id/mahasiswa/plugins/bootstrap-wysihtml5/text/  (Not Found)
ᔓᔓ Finished after 16 seconds
No interesting files detected ¯\_(ツ)_/¯
```

Gambar 4.36 Hasil Analisa Hidden Directory Objek Penelitian Dirhunt 3 Tools

Berdasarkan hasil data yang disampaikan oleh *tools* dirhunt, ditemukan sebuah informasi mengenai kondisi status dari masing masing *directory* dan status index pada beberapa directory. Salah satu fitur atau kelebihan dari *tools* dirhunt adalah bisa mendeteksi status *directory* yang di *redirect* oleh situs *web*. Dengan adanya informasi tersebut seorang penguji *(penetration tester)* bisa mendapatkan gambaran mengenai file index apa saja yang ada pada objek penelitian. Hal tersebut bisa dilakukan analysis pada tahap selanjutnya. Namun hasil kali ini yang ditemukan oleh tools dirhunt pada objek penelitian belum mendapatkan informasi sensitif pada objek penelitian seperti yang ditunujukan pada Gambar 4.36.

4.2.3 Vulnerability Assement

Berdasarkan data yang diperoleh dari pengembang, *vulnerability assement* merupakan penganalisaan data yang didapatkan pada fase "*Reconnaisance*" untuk mengidentifikasi kemungkinan celah dan teknik pada exploitasinya. *Vulnerability assement* pada penelitian ini dilakukan dengan beberapa tahap. Tahap pertama menggunakan analisa yang dilakukan oleh penulis / penguji. Tahap kedua menggunakan *vulnerability scanner tools* .Berikut data *vulnerability assement* yang diperoleh dari objek penelitian.

A. Vulnerability assement berdasarkan analisa penulis/penguji

Pada tahap ini penguji melakukan analisa berdasarkan data yang didapatkan pada tahap *reconnaisnace*. Berikut data *vulnerability assessment* berdasarkan analisa penulis atau penguji. Seperti yang ditujukan pada Tabel 4.2.

Tabel 4.2 List Vulnerability Assement

Vulnerability Assement/ Vulnerability Analysis							
		Type Of Reconnasisance					
	Tools	*Passive*	*Active*	*Sensitive Information*	*Location*	*Potential of Attack*	*Risk Level*
Reconnaisance Phase	Netcraft(*Integrated* virus total) Nikto	✓	✓	Mengenai X-XSS protection yang dijelaskan terdapat filter atau keamanan anti XSS. Tidak ditemukan/ditentukan XSS protection Ditemukan tautan berisi informasi sensitif	Header Port 80 Port 443		

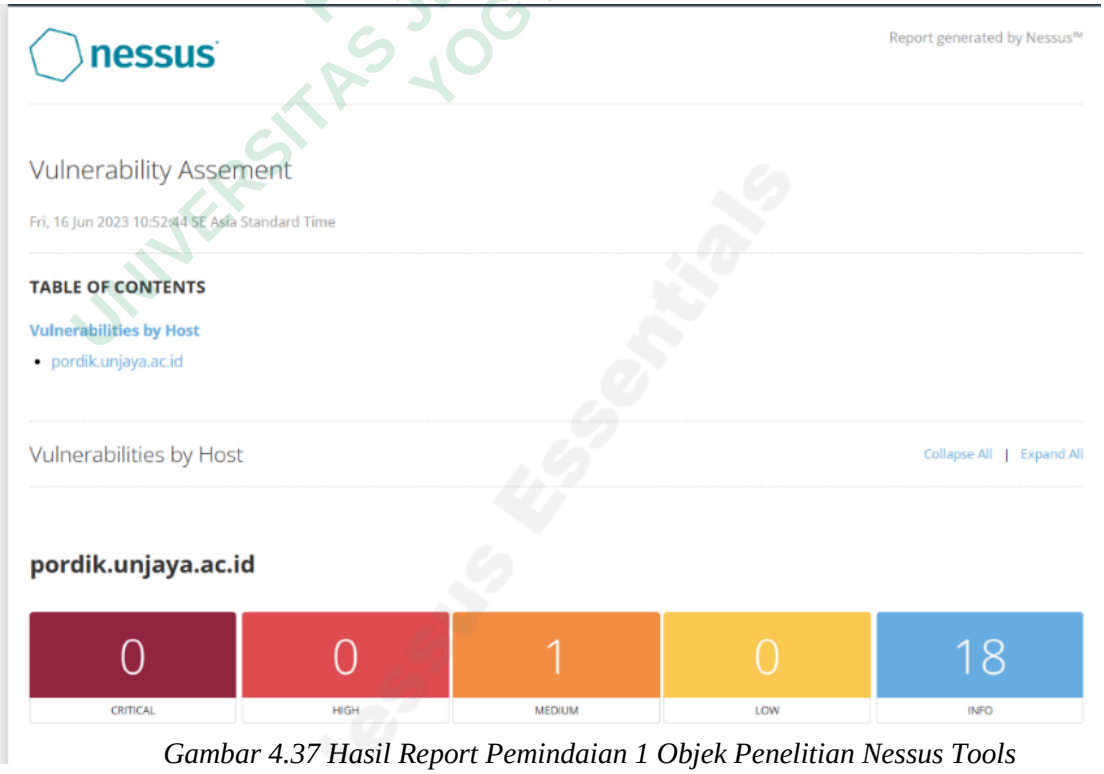
Vulnerability Assement/ Vulnerability Analysis							
		Type Of Reconnasisance					
	Tools	*Passive*	*Active*	*Sensitive Information*	*Location*	*Potential of Attack*	*Risk Level*
Reconnaisance Phase	WPScan		✓	Ditemukan celah serangan "breach attack" Tidak ditemukan anti click jacking pada X frame – option header Ditemukan 21 *vulnerable* pada Wordpress version 6.0.1 Ditemukan *the version out of date* pada *theme* wordpress (versi kadaluarsa)	Server Header *Plugin* wordpess yang digunakan insecure *Theme* WordPress, yang terupdate 1.2.9		

Vulnerability Assement/ Vulnerability Analysis							
		Type Of Reconnasisance					
	Tools	*Passive*	*Active*	*Sensitive Information*	*Location*	*Potential of Attack*	*Risk Level*
Reconnaisance phase	Dirsearch		✓	Ditemukan tautan wp admin pada objek penelitian	https://pordik.unjaya.ac.id/wp-login.php yang terdirect https%3A%2F%2Fpordik.unjaya.ac.id%2Fwp-admin%2&reauth=1		
	Google dork/GHDB	✓		Ditemukan informasi 3 informasi log in: Login mahasiswa, dosen dan orang tua	Pada "site" *website* objek penelitian		
	Nmap		✓	Ditemukan port yang terbuka yaitu port 80,443,8081,53	Nmap output kernel kali linux http.https, blackice-icecap,UDP		

B. *Vulnerability assement* menggunakan tools nessus

Berikut data vulnerability assement menggunakan tools nessus yang dilakukan pada objek penelitian.

Dari hasil yang ditemukan dari objek penelitian menggunakan domain menggunakan *tools* dari Nessus, terdapat beberapa kerentanan. Pada Nessus terdapat beberapa tingkatan kategori kerentanan yang ditandai dengan *icon* warna yang berbeda. *Icon* warna biru menunjukan *Info*, warna kuning menunjukan *Low*, warna *orange* menunjukan*Medium*,warna merah menunjukan *High*, warna merah tua menunjukan *Critical* dan warna ungu menunjukan *Mixed* yaitu terdapat beberapa kategori risiko yang berada dalam satu kelompok. Tingkatan risiko tersebut juga terdapat tabel yang berupa informasi data yang telah diolah oleh Nessus untuk mempermudah dalam analisis pengolahan data. Berikut hasil pemindaian kerentanan dari ketiga IP berdasarkan kategori tingkat risiko. Seperti ditujukan pada Gambar 4.37 dan Gambar 4.38



Gambar 4.37 Hasil Report Pemindaian 1 Objek Penelitian Nessus Tools

Severity	CVSS v3.0	VPR Score	Plugin	Name
MEDIUM	5.0*	-	90067	WordPress User Enumeration
INFO	N/A	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	40406	CGI Generic Tests HTTP Errors
INFO	N/A	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	49704	External URLs
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	91634	HyperText Transfer Protocol (HTTP) Redirect Information
INFO	N/A	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	91815	Web Application Sitemap
INFO	N/A	-	49705	Web Server Harvested Email Addresses
INFO	N/A	-	10386	Web Server No 404 Error Code Check

Gambar 4.38 Hasil Report Pemindaian 2 Objek Penelitian Nessus Tools

Berdasarkan data yang diperoleh dari tools nessus ditemukan tingkat kerentanan pada level *MEDIUM* yang mengacu pada CVSS *(Common Vulnerability Scoring System)* v3.0. Tingkat kerentanan tersebut terletak pada WordPress User Enumeration. Seperti yang ditunjukan pada Gambar 4.38.

C. *Vulnerability assement* menggunakan *tools* wpscan

Melihat kerentanan pada situs web objek penelitian menggunakan vulnerability scanner *WPScan*

```
[+] WordPress version 6.0.1 identified (Insecure, released on 2022-07-12).
 | Found By: Rss Generator (Passive Detection)
 |  - https://pordik.unjaya.ac.id/?feed=rss2, <generator>https://wordpress.org/?v=6.0.1</generator>
 |  - https://pordik.unjaya.ac.id/?feed=comments-rss2, <generator>https://wordpress.org/?v=6.0.1</generator>
 |
 | [!] 21 vulnerabilities identified:
 |
 | [!] Title: WP < 6.0.2 - Reflected Cross-Site Scripting
 |     Fixed in: 6.0.2
 |     References:
 |      - https://wpscan.com/vulnerability/622893b0-c2c4-4ee7-9fa1-4cecef6e36be
 |      - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
 |
 | [!] Title: WP < 6.0.2 - Authenticated Stored Cross-Site Scripting
 |     Fixed in: 6.0.2
 |     References:
 |      - https://wpscan.com/vulnerability/3b1573d4-06b4-442b-bad5-872753118ee0
 |      - https://wordpress.org/news/2022/08/wordpress-6-0-2-security-and-maintenance-release/
```

Gambar 4.39 Hasil Scanning 1 Objek Penelitian WPScan

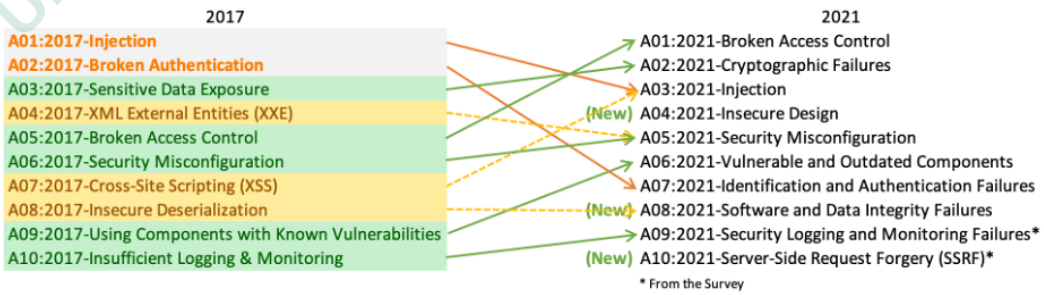
```
[+] WordPress theme in use: blossom-spa
 | Location: https://pordik.unjaya.ac.id/wp-content/themes/blossom-spa/
 | Last Updated: 2022-09-19T00:00:00.000Z
 | Readme: https://pordik.unjaya.ac.id/wp-content/themes/blossom-spa/readme.txt
 | [!] The version is out of date, the latest version is 1.2.9
 | Style URL: https://pordik.unjaya.ac.id/wp-content/themes/blossom-spa/style.css?ver=1.2.8
 | Style Name: Blossom Spa
 | Style URI: https://blossomthemes.com/wordpress-themes/blossom-spa/
 | Description: Blossom Spa is a clean and beautiful WordPress Theme focused on Spa and Salon business. You can use ...
 | Author: Blossom Themes
 | Author URI: https://blossomthemes.com/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.2.8 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://pordik.unjaya.ac.id/wp-content/themes/blossom-spa/style.css?ver=1.2.8, Match: 'Version: 1.2.8'
```

Gambar 4.40 Hasil Scanning 2 Objek Penelitian WPScan

Berdasarkan penggunaan *tools* WPScan pada objek peneleitian memberikan sebuah informasi sebagai berikut.

a. Wordpress *version* yang digunakan pada objek penelitian mengguanakan version 6.0.1 dirilis pada 07-12-2022, seperti ditujukan pada Gambar 4.39, Gambar 4.40.
b. Wordpress *version* 6.0.1 memiliki 21 jenis kerentanan yang ditemukan, seperti ditujukan pada Gambar 4.39
c. Beberapa kerentanan masuk dalam kategori OWASP (*Open Web Application Project)* Top 10 2021 yaitu, *cross site scripting* (XSS) yang sekarang menjadi bagian dari kategori Injection (OwaspTop10, 2021) .

   Seperti yang ditujukan pada Gambar 4.41.



Gambar 4.41 Cartegory OWASP TOP 10 Update 2021

D. Vulnerability assement menggunakan tools burpsuite

Gambar 4.42 Vulnerability Scanner 1 Objek Penelitian Burp Suite Tools

Gambar 4.43 Vulnerability Scanner 2 Objek Penelitian Burp Suite Tools

Berdasarkan data *vulnerability assement* menggunakan tools burpsuite pada objek penelitian dalam *web application* ditemukan sebuah celah. Celah yang ditemukan pada *framework* yang berversi 3.3.6. Adapun anomali yang ditemukan pada *framework* tersebut terdapat celah XSS *(cross site scripting*) (Snyk, 2023). Seperti pada Gambar 4.42 dan Gambar 4.43.

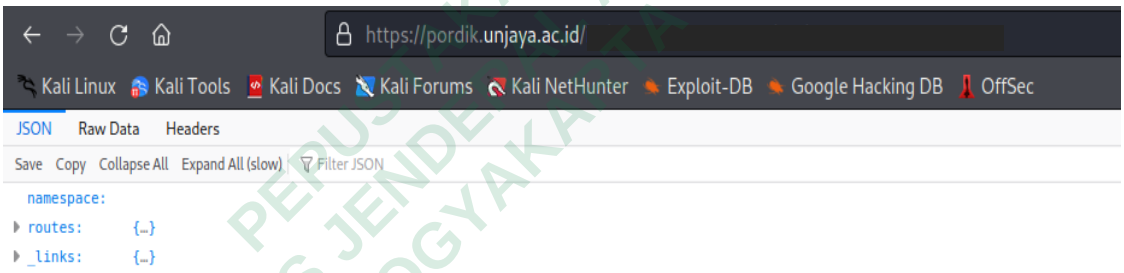
4.2.4 Exploitation

Pada fase ini akan dilakukan pengujian celah keamanan pada objek penelitian, berdasarkan informasi yang didapatkan pada fase *vulnerability assement* dengan menggunakan *tools* yang sudah ditentukan.

Berikut fase *exploitation* pada objek penelitian.

A. *Eavesdropping*

Pengujian pada fase *exploitasi* yang ditemukan dengan melakukan scanning dengan mencari *vulnerability* pada objek penelitian, ditemukan infromasi *sensitive* menggunakan *tools* Nikto. Adapun informasi yang tersebut, informasi *sensitivie* pada API dan anomaly celah XSS *(cross site scripting)* yang dapat dieksekusi. Seperti pada Gambar 4.44



Gambar 4.44 Exploit , Sensitive Information 1 Objek Penelitian NIkto Tools

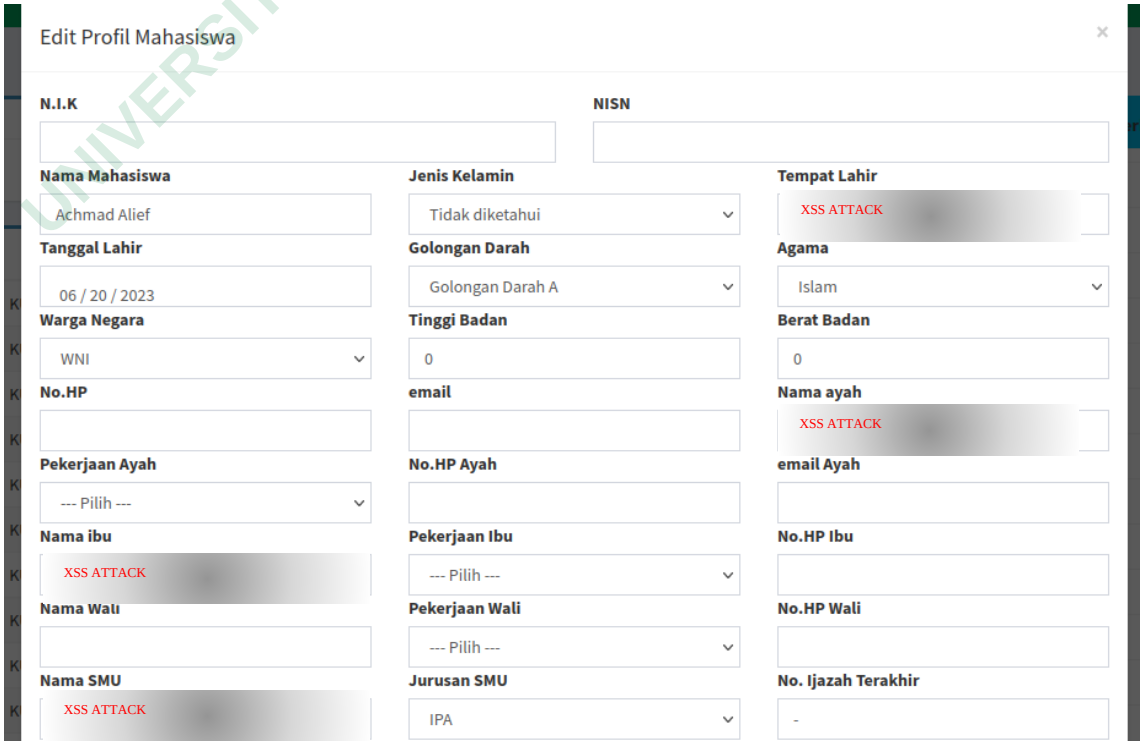
Pengujian terhadap kelemahan pada *web server* ketika mentransimiskan data menggunakan nikto *tools*.

Hasil dari proses vulnerability scanner yang dilakukan pada fase *exploitasi*, didapatkan informasi celah keamann pada API pada objek penelitian. Salah satu celah keamanan informasi tersebut memberikan data bahwa pada situs web terdapat 2 admin yang mengelola sistem informasi pada situs web. Hal tersebut merupakan informasi *sensitive* yang seharusnya tidak terlihat secara publik. Seperti pada Gambar 4.45

Gambar 4.45 Exploit , Sensitive Information 2 Objek Penelitian Burpsuite Tools

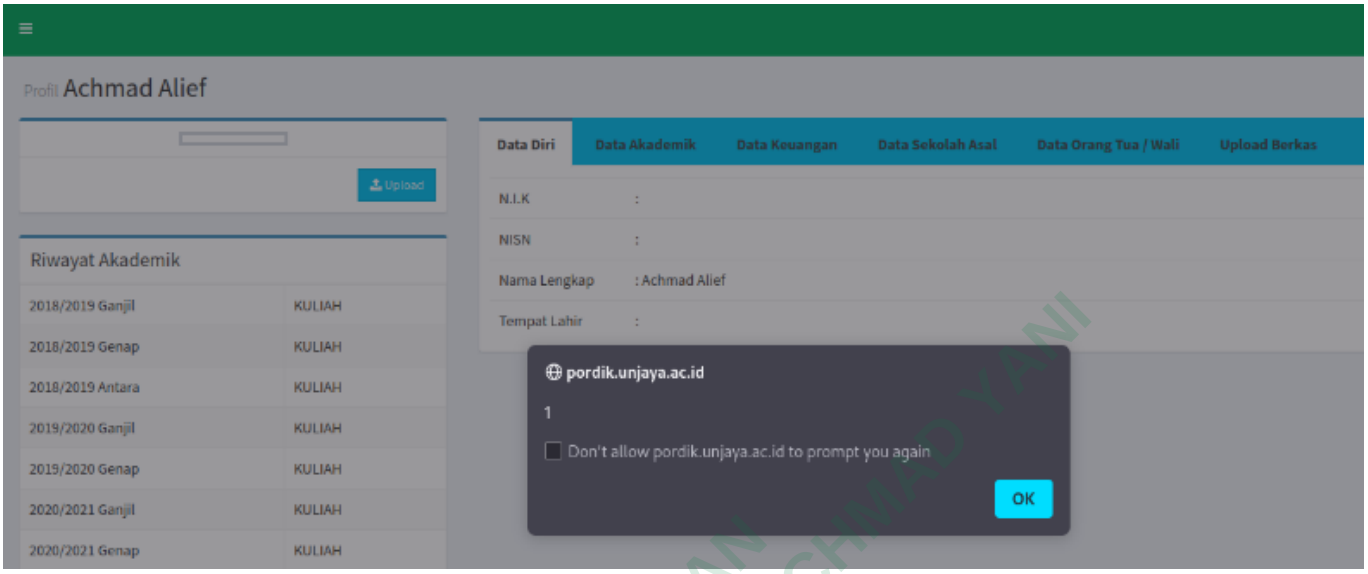
B. XSS (*cross site scripting*)

Pengujian pada fase *exploitation* yang ditemukan dengan mencari kerentanan terhadap serangan XSS *(cross site scripting)* dengan menggunakan *tools* burpsuite. Terdapat 1 vektor serangan yang dilakukan pada *web app* pada objek penelitian yaitu, pada *web app* mahasiswa seperti pada Gambar 4.46



Gambar 4.46 Exploit, Vektor(Payload) XSS Attack Objek Penelitian Technical Tools

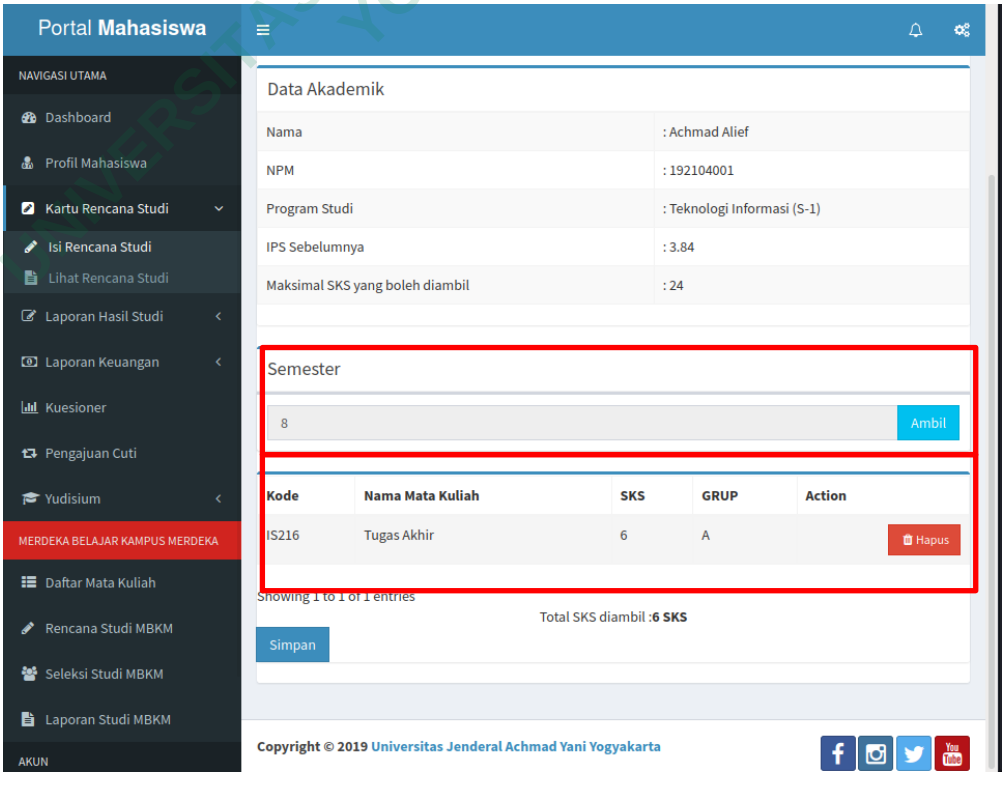
Berikut hasil dari XSS *attack* yang dilakukan seperti pada Gambar 4.47



Gambar 4.47 Exploit, Result XSS Attack Objek Penelitian

C. *Business Logic Vulnerability*

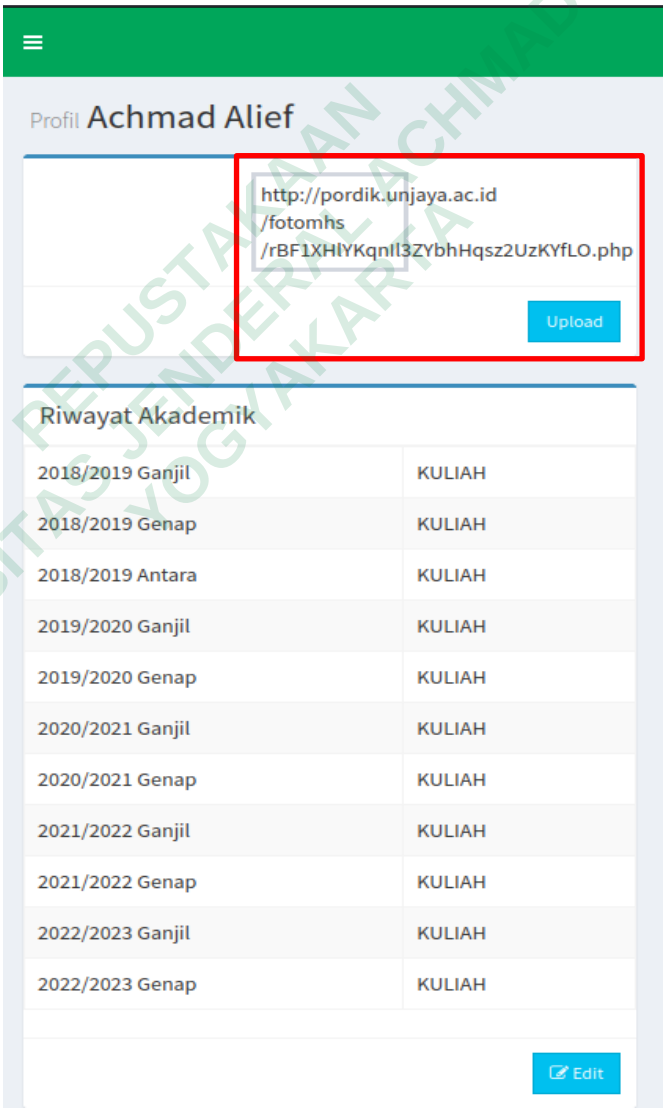
Pengujian pada fase *exploitation* yang ditemukan dengan menganalisa karakteristik pada situs *web* objek penelitian. Berikut *Business Logic Vulnerability* yang ditemukan seperti pada Gambar 4.48



Gambar 4.48 Exploit, Result Business Logic Attack Objek Penelitian Burp Suite Tools

D. *File Upload Vulnerability*

Hasil pengujian pada fase *exploitation* yang ditemukan, dengan mencoba melakukan serangan mengupload suatu file yang tidak seharusnya pada form upload profil mahasiswa menemukan sebuah anomali. Hal tersebut dilakukan untuk melihat bagaimana respon dari webserver setelah menerima file tersebut. Hasilnya pada form upload mahasiswa ditemukan sebuah celah *unrestricted attack vulnerability*. Berikut hasil *unrestricted attack vulnerability* yang ditemukan pada Gambar 4.49



Gambar 4.49 Exploit, Result unrestricted attack Objek Penelitian Burp Suite Tools

4.2.5 Reporting

Tahap ini merupakan tahap akhir dari seluruh fase pengujian pada objek penelitian menggunakan metode pendeketan PTES (*Penetration Testing Execution Standard*). Berdasarkan data tersebut penulis atau penguji bisa mengambil kesimmpulan dari hasil pengujian pada situs *web* objek penelitian, yang ditujukan pada Tabel 4.3

Tabel 4.3 Hasil Pengujian Penetration Testing

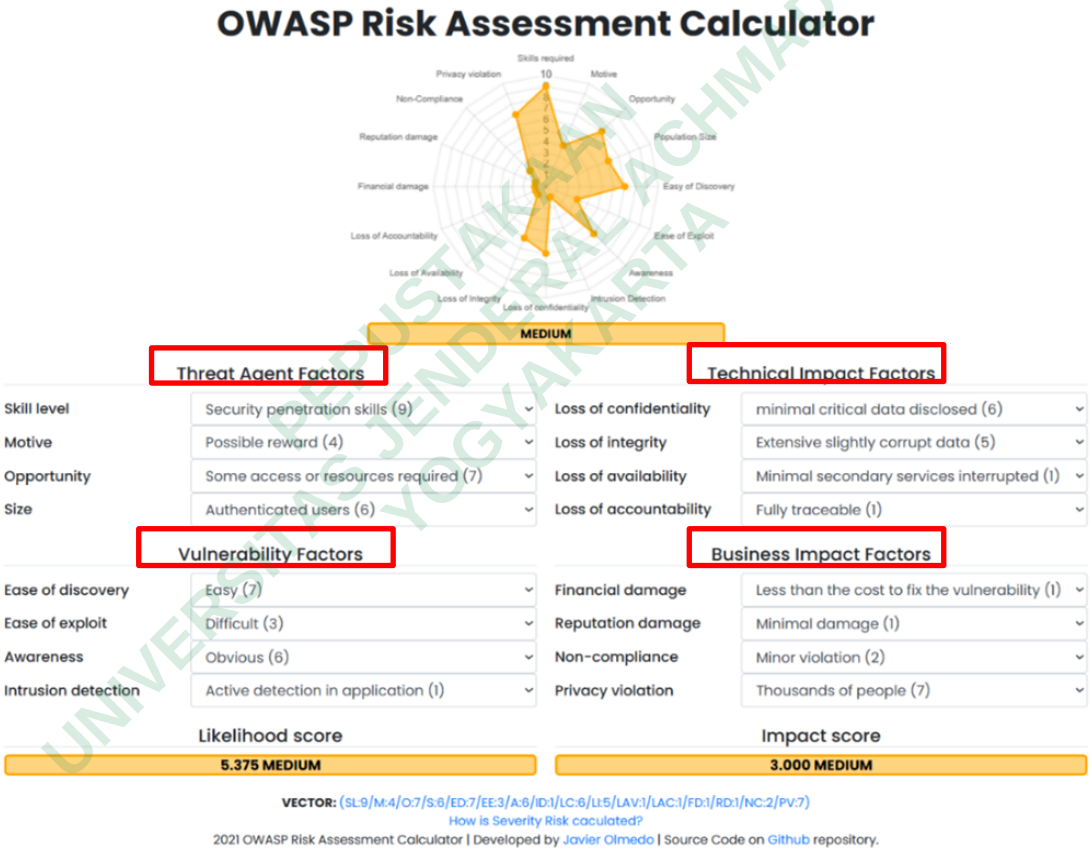
Jenis Serangan	**Tools**	**Status**
Eavesdropping	Burpsiuite	Berhasil
		Berhasil
Cross Site Scripting	Burpsuite	Berhasil
Businsess Logic	Burpsuite	Berhasil
File Upload Vulnerability	Burpsuite	Berhasil

Berdasarkan dari ke 4 serangan yang diketahui pada tahap exploitation semuanya berhasil. Serangan tersebut, *Eavesdropping*, XSS (*Cross Site Scripting*), *Businsess Logic dan File Upload Vulnerability*. Berikut kategori dan profil resiko berdasarkan standard OWASP Top 10 seperti pada Tabel 4.4

Tabel 4.4 Hasil Pengkategorian Referensi OWASP TOP 10 2021

OWASP TOP 10 2021 Category				
Jenis Serangan	*Eavesdropping*	*Cros site scripting*	*Businsess Logic Vulnerability*	*File Upload Vulnerability*
List Category	*A05 Security Missconfiguration*	*A03 Injection*	*A04 Insecure Design*	*A07 Identi & Autehen Failures*
Profil Resiko	*MEDIUM*	*CRITICAL*	*HIGH*	*CRITICAL*

Berikutnya assement tingkat resiko keamanan terhadap *website* layanan Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta berdasarkan OWASP Risk Assement Calculator 2021. Berdasarkan dari rangkaian tahap pengujian untuk menentukan *OWASP Risk Rating* dari ancaman tersebut ada beberapa tahapan dapat menentukan berapa besarnya resiko yang akan muncul, tahapan tersebut merupakan *Threat Agent Factors, Vulnerability Factors, Technical Impact, Business Impact.* Berikut *result* data assement tingkat resiko keamanan situs *web* layanan Portal Akademik Universitas Jenderal Achmad Yani Yogyakarta seperti pada Gambar 4.50.



Gambar 4.50 OWASP Risk Assement Calc pada objek penelitian

Berdasarkan *auto calculate* yang dilakukan, dapat diambil kesimpulan bahwasannya tingkat resiko keamanan pada objek penelitian berada dilevel *MEDIUM*. Hal tersebut menjadi suatu perhatian khusus yang perlu ditindak lebih lanjut untuk meminimalisir terjadinya serangan dari pihak yang tidak bertanggung jawab.