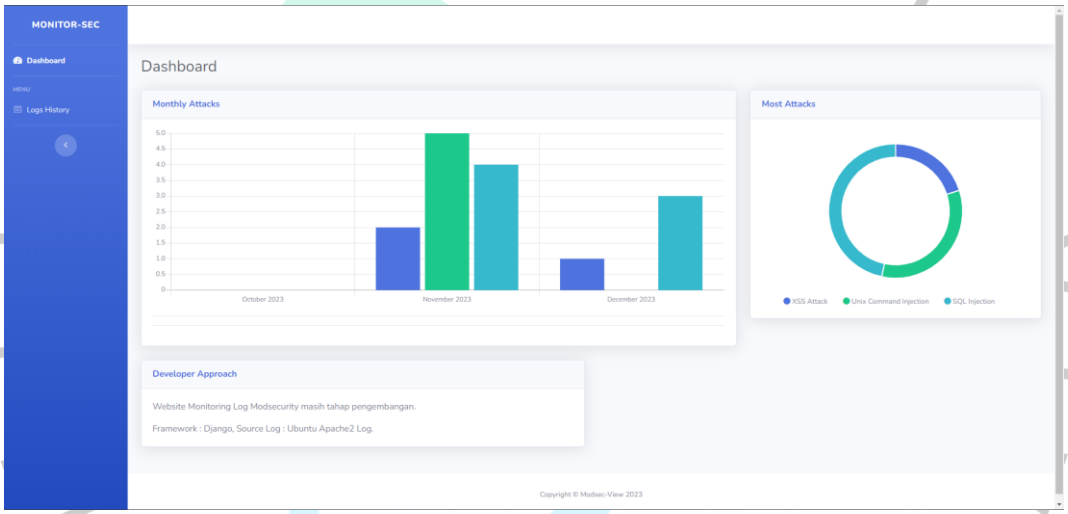
BAB V
HASIL DAN PEMBAHASAN

Setelah melalui fase perencanaan penelitian, pengembangan sistem ini harus diuji terlebih dahulu sebelum diluncurkan, untuk memastikan apakah sistem dapat berfungsi sesuai dengan tujuan dan metode yang telah ditetapkan atau tidak. Hal ini dilakukan untuk melihat hasil yang telah dicapai.

5.1 Hasil

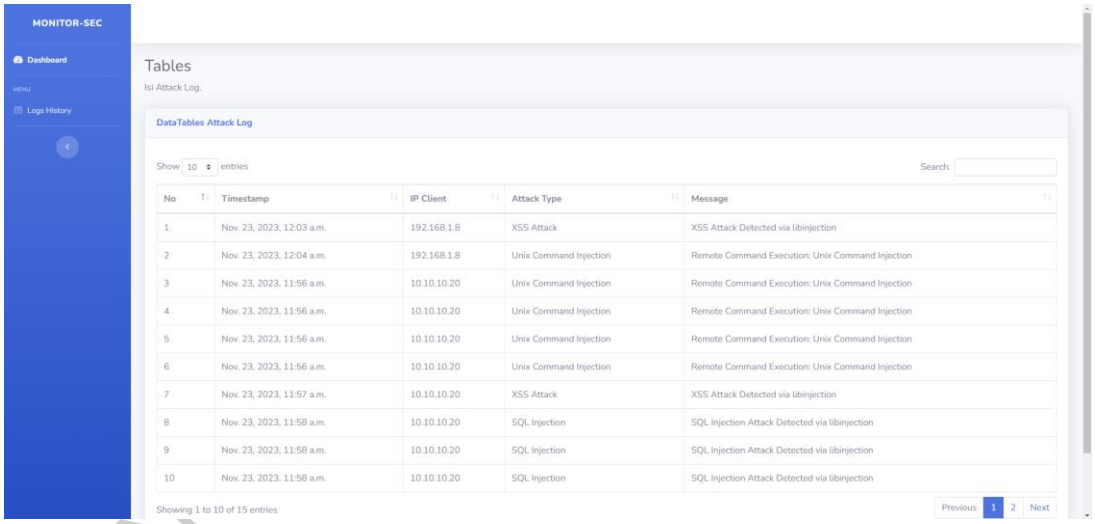
Hasil yang diperoleh pada pengembangan ini meliputi hasil implementasi rancangan antar muka dan implementasi *modsecurity*

5.2.1 Hasil Implementasi Rancangan Antar Muka



Gambar 5. 1 Halaman *Dashboard*

Gambar 5.1 menunjukkan halaman utama website yang telah dibuat. Pada halaman utama terdapat dua jenis informasi, jumlah serangan masuk dan jumlah serangan bulanan ke aplikasi *web*.



Gambar 5. 2 Halaman Histori *Log*

Gambar 5.2 menunjukkan halaman Histori Log yang telah dibuat. Halaman ini berisikan informasi identitas dan pesan dari modsecurity bila ada attackeran ke website.

5.2.2 Hasil Implementasi Metode Pengembangan *DevOps*

Pada bab sebelumnya dijelaskan metode pengembangan *DevOps* yang termasuk dalam metode pengembangan aplikasi *monitoring* ini. Berikut merupakan hasil implementasi yang telah dilakukan.

1. ***Fase* 1 : Perencanaan Dan Analisis**
   - **Menentukan Kebutuhan**

     Kebutuhan yaitu berfokus pada mengambil data *log modsecurity* yang masuk diintegrasikan dengan *Django* dan *Telegram*.
   - **Memilih Alat *DevOps***

     Alat yang digunakan untuk pengembangan adalah *GitHub* yaitu untuk mengontrol versi dengan pembaruan secara berkala.
2. ***Fase* 2 : Pengembangan**
   - **Mengatur Lingkungan Kebutuhan**

     Lingkungan yang digunakan yaitu *Ubuntu* 22.04 Live Server untuk *Modsecurity* dan *Web Server*, sedangkan untuk pembuatan aplikasi menggunakan *tools Visual Studio Code* pada *Framework Django*.
   - **Pengembangan Berbasis *Fitur***

     Pengembangan dilakukan secara *iterative*, dengan menggunakan *Git*
   - ***Code review***

Setiap kode yang sudah dikerjakan secara bertahap, digunakanlah fitur Git Pull untuk melihat kualitas kode.

3. ***Fase* 3 : Pengujian**
   - **Otomasi pengujian**

     Implementasi otomisasi menggunakan daemon dari Ubuntu yang mempunyai fungsi menjalan skrip otomatis selama sistem dihidupkan.
   - **Integrasi terus-menerus**

     Setiap kode parsing dan notifikasi intrusi dilakukan pengujian otomatis untuk melihat berapa efektif jika dijalankan dan mendapatkan data.
4. ***Fase* 4 : Peluncuran**
   - ***Deployment***

     Sistem ini ditempatkan pada direktori *Ubuntu* dan dijalankan melalui *virtualenv* yang dimiliki *Server*. Jika kode tidak ada masalah akan ditempatkan pada *daemon-services* supaya berjalan otomatis.
5. ***Fase* 5 : Operasi dan Pemantuan**
   - **Pengaturan Pemantauan**

     Alat digunakan untuk memantau infrastruktur jika semua *service* dijalankan yaitu melalui *web console* Grafana walau tidak termasuk dalam inti aplikasi, *Grafana* sangat berguna untuk melihat kemampuan sistem Ubuntu.
   - ***Logging* dan Analisis**

     Log yang digunakan berasal dari *Apache2* yaitu *error*. *Log* ini berisikan informasi yang dimuat dalam satu *file* dan mencatat cukup lengkap untuk *logging Modsecurity*.
6. ***Fase* 6 : Evaluasi dan Perbaikan**
   - ***Feedback Loop***

     Ketika sistem berjalan dan pemantauan log yang sudah berhasil diparsing jika ada kendala dapat dilakukannya perbaikan.
   - **Iterasi**

     Sistem ini selalu menerapkan perbaikan dan memperbarui konfigurasi secara berkala agar sistem dapat berjalan dengan semestinya.

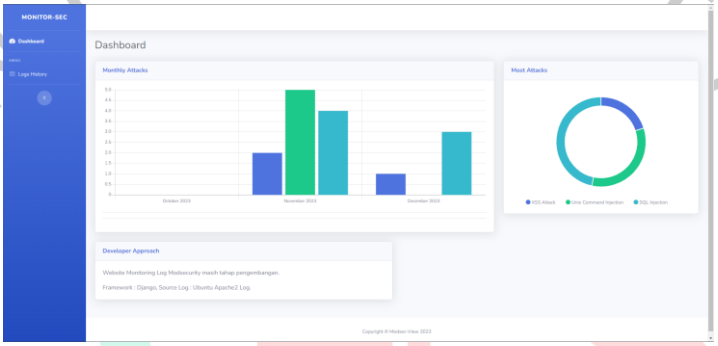
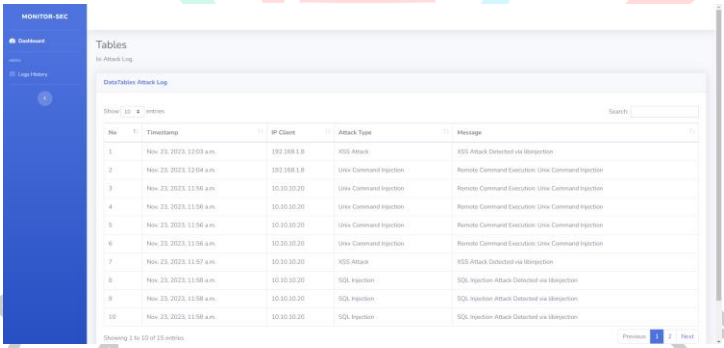
5.3 Pembahasan

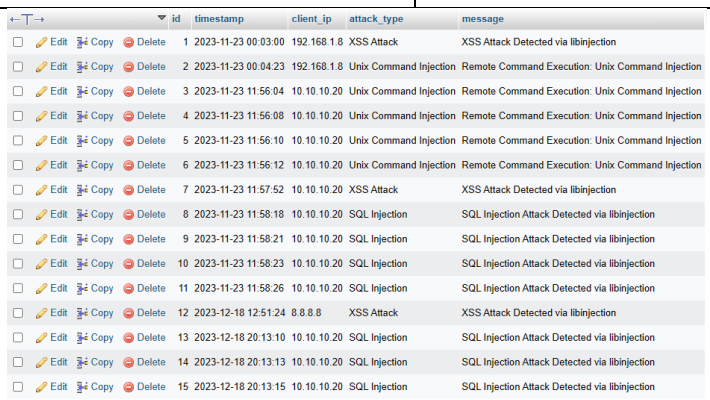
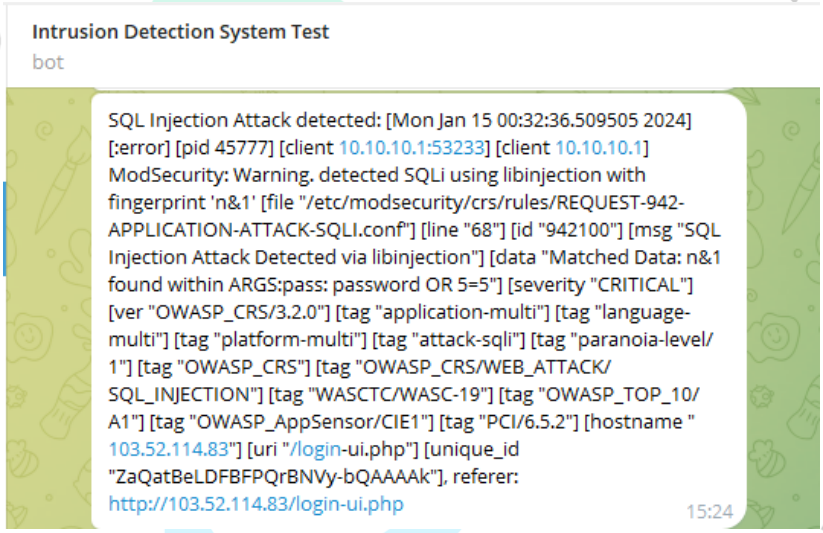
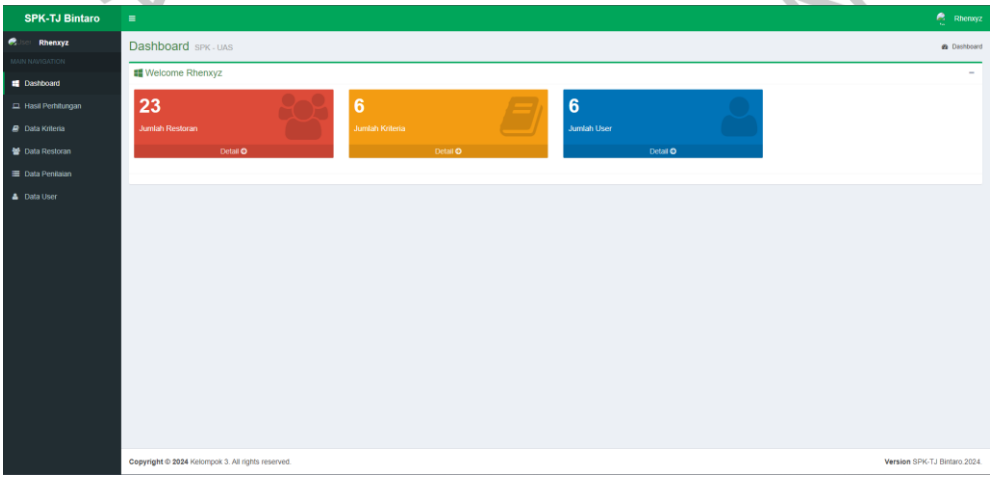
Pada sub-bab pembahasan, peneliti akan menjelaskan secara detail hasil keseluruhan dari sub-bab sebelumnya dan memberikan kesimpulan dari hasil yang telah diperoleh.

5.3.1 Pengujian *Black box*

Metode pengujian *black box* digunakan untuk menganalisis fungsionalitas suatu perangkat lunak atau aplikasi tanpa memerlukan pengetahuan khusus tentang kode program yang digunakan.

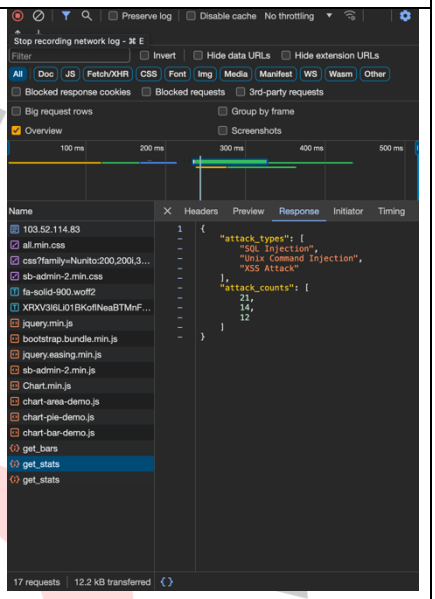
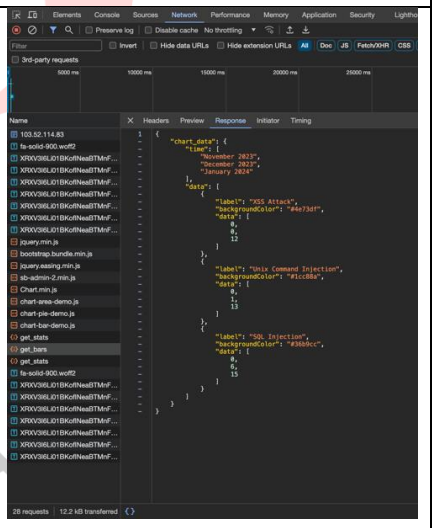
Tabel 5.1 Pengujian *Blackbox*

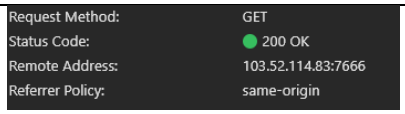
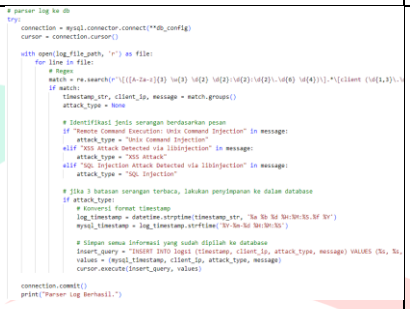
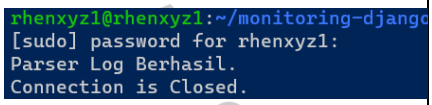
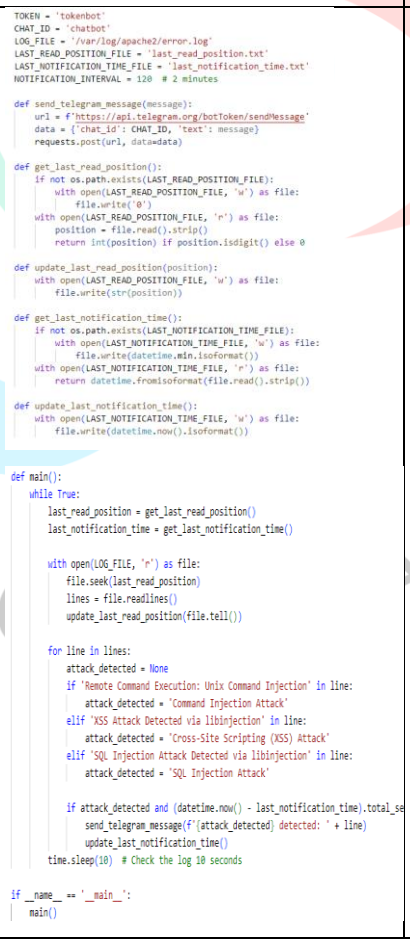
No	Skenario Pengujian	Hasil yang diharapkan
1	Dashboard	User dapat mengakses halaman utama
Hasil Pengujian 		
2	Histori Log	User dapat melakukan akses halaman Histori *Log*
Hasil Pengujian 		
3	*Skrip Parsing Log*	Kode dapat mengekstrak *log* untuk disimpan ke *database*
Hasil Pengujian		

No	Skenario Pengujian	Hasil yang diharapkan
		
4	Skrip *telegram bot*	Kode dapat mengirimkan notifikasi intrusi ke *telegram*
Hasil Pengujian 		
6	Akses halaman objek	User dapat mengakses halaman objek untuk melakukan tes serangan
Hasil Pengujian 		

5.3.2 Pengujian *white box*

Tabel 5. 2 Pengujian *White box*

No.	Hasil yang diharapkan	Source Code	Hasil Pengujian
1	*Pie chart* mendapatkan data dari db untuk divisualisasikan sebagai *'most attacks'*	`function fetchDataAndUpdateChart() { $.ajax({ url: "get_stats", // Replace with the actual API endpoint method: 'GET', success: function(res) { // Assuming the server returns an array of data points chartData(res) }, error: function(error) { console.error('Error fetching data:', error); } }); } setInterval(fetchDataAndUpdateChart(), 1500);`	
2	*Bar Chart* mendapatkan data dari db untuk divisualisasikan bagian "*monthly attacks*"	`function fetchBars() { $.ajax({ url: "get_bars", // Replace with the actual API er method: 'GET', success: function(res) { // console.log(res.chart_data.data) // Assuming the server returns an array of data let ctx = document.getElementById("myBarChart") let myBarChart = new Chart(ctx, { type: 'bar', data: { labels: res.chart_data.time, // Menggunaka datasets: res.chart_data.data } }); }, error: function(error) { console.error('Error fetching data:', error); } }); }`	

No.	Hasil yang diharapkan	Source Code	Hasil Pengujian
3	Akses halaman Histori *Log* dan mendapat data dari *database*		
4	Skrip *parsing log* agar masuk dan sudah dipilah ke dalam *database*		
5	Skrip notifikasi intrusi melalui *Telegram*		

5.3.3 Hasil analisis modsecurity

Hasil yang diperoleh modsecurity dalam menangani serangan pada aplikasi (objek) yang menggunakan tools ZAP-OWASP sebagai berikut.

Tabel 5. 3 Hasil yang diperoleh *modsecurity*

Kategori Serangan	Jumlah Serangan	Objek Serang
Command Injection	54 hit	Aplikasi web dev
SQL Injection	77 hit	
Cross-site Scripting	8 hit	

Untuk menciptakan *confidence score* dari hasil analisis OWASP-ZAP yang dilakukan, peneliti perlu menetapkan beberapa kriteria dan indikator. Karena data yang peneliti miliki didasarkan pada ekspor alat-alat ini, peneliti menggunakan pendekatan sederhana berdasarkan informasi yang tersedia.

Metrik untuk *confidence score.*

1. Kode Status HTTP: Kode dari HTTP sebagai indikator utama yaitu status 403 dapat diakui sebagai indikasi kepercayaan tertinggi bahwa serangan dapat dicegah oleh Modsecurity.
2. Jenis Metode Permintaan: Permintaan ‘POST’ banyak digunakan untuk penyerangan, dan ‘GET’ biasa digunakan untuk pengambilan data. Peneliti memberi bobot lebih tinggi pada permintaan ‘POST’ dalam menentukan *confidence score*.
3. Frekuensi Permintaan yang Sama: Jika ada indikasi permintaan URL yang sama berulang kali dengan hasil 403 (*Forbidden*), ini dapat meningkatkan *confidence score* bahwa ada upaya telah dilakukannya penyerangan terhadap *website*.

Pembuatan Skor

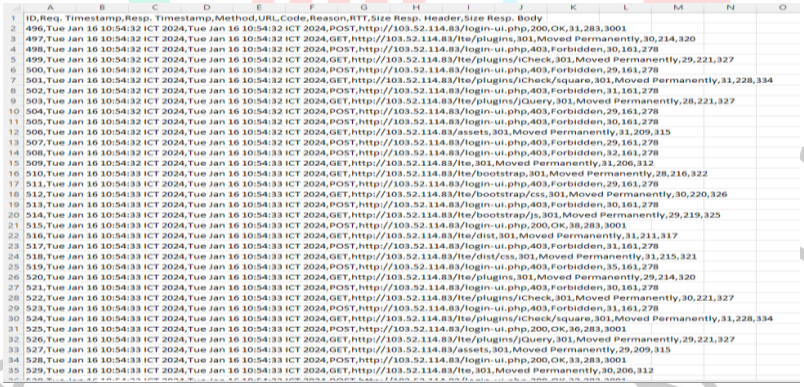
- Skor awal: Setiap permintaan dimulai dari 0.
- Kode Status 403: 50 poin untuk status 403.
- Metode ‘POST’: 30 poin jika permintaan adalah ‘POST’
- Metode ‘GET’: 20 poin jika permintaan adalah ‘GET’.
- Frekuensi Permintaan: 20 poin untuk permintaan yang berulang.

Skor maksimum yang ditentukan ada 100. Peneliti menghitung skor untuk beberapa data untuk diterapkan. Berikut merupakan tabel untuk *confidence score* pada log yang dihasilkan modsecurity:

Tabel 5. 4 *Confidence score* pada *log*

URL	Metode	Kode	Confidence Score
http://103.52.114.83/lte/plugins/ iCheck/square/	GET	403	70
http://103.52.114.83/lte/plugins/jQuery/	GET	403	70
http://103.52.114.83/login-ui.php	POST	403	80
http://103.52.114.83/login-ui.php	POST	403	80
http://103.52.114.83/login-ui.php	POST	403	80

Pada tabel 5.4, setiap permintaan (POST/GET) mendapat skor yang berdasarkan kriteria yang ditetapkan. Ini menunjukkan confidence yang cukup tinggi bahwa penyerangan terhadap website dapat dicegah. Data ini di dukung oleh log yang dihasilkan oleh modsecurity dan di visualisasikan pada aplikasi monitoring.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	ID,Req. Timestamp,Resp. Timestamp,Method,URL,Code,Reason,RTT,Size Resp. Header,Size Resp. Body														
2	496,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,POST,http://103.52.114.83/login-ui.php,200,OK,31,283,3001														
3	497,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,GET,http://103.52.114.83/lte/plugins,301,Moved Permanently,30,214,320														
4	498,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,30,161,278														
5	499,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,GET,http://103.52.114.83/lte/plugins/iCheck,301,Moved Permanently,29,221,327														
6	500,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,29,161,278														
7	501,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,GET,http://103.52.114.83/lte/plugins/iCheck/square,301,Moved Permanently,31,228,334														
8	502,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,31,161,278														
9	503,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,GET,http://103.52.114.83/lte/plugins/jQuery,301,Moved Permanently,28,221,327														
10	504,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,29,161,278														
11	505,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,30,161,278														
12	506,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,GET,http://103.52.114.83/assets,301,Moved Permanently,31,209,315														
13	507,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:32 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,29,161,278														
14	508,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,32,161,278														
15	509,Tue Jan 16 10:54:32 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte,301,Moved Permanently,31,206,312														
16	510,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/bootstrap,301,Moved Permanently,28,216,322														
17	511,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,29,161,278														
18	512,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/bootstrap/css,301,Moved Permanently,30,220,326														
19	513,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,30,161,278														
20	514,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/bootstrap/js,301,Moved Permanently,29,219,325														
21	515,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,200,OK,38,283,3001														
22	516,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/dist,301,Moved Permanently,31,211,317														
23	517,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,31,161,278														
24	518,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/dist/css,301,Moved Permanently,31,215,321														
25	519,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,35,161,278														
26	520,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/plugins,301,Moved Permanently,29,214,320														
27	521,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,30,161,278														
28	522,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/plugins/iCheck,301,Moved Permanently,30,221,327														
29	523,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,403,Forbidden,31,161,278														
30	524,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/plugins/iCheck/square,301,Moved Permanently,31,228,334														
31	525,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,200,OK,36,283,3001														
32	526,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte/plugins/jQuery,301,Moved Permanently,29,221,327														
33	527,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/assets,301,Moved Permanently,29,209,315														
34	528,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,POST,http://103.52.114.83/login-ui.php,200,OK,33,283,3001														
35	529,Tue Jan 16 10:54:33 ICT 2024,Tue Jan 16 10:54:33 ICT 2024,GET,http://103.52.114.83/lte,301,Moved Permanently,30,206,312														

Gambar 5. 3 csv excel

Gambar 5. 4 export ZAP log Modsecurity