|  |
| --- |
| 1. **INCIDENT REPORT FORM** |

|  |  |
| --- | --- |
| **I. Identitas Pelapor & Bukti Insiden (\*)** | |
| Kategori Insiden (*category of incident*) : | Jenis insiden :   1. **web defacement** 2. **hacking** 3. ~~malware detection~~ 4. ~~phising~~ 5. ~~spoofing~~ 6. ~~brute force~~ 7. ~~denial of service~~ 8. ~~sniffing~~ 9. ~~lainnya :~~ |
| (\*) Catatan : pilih salah satu atau lebih kategori insiden di atas |
| Pelapor (*incident report by*) : | Tanggal Laporan : 16-07-2020  Nama : ………………………..  Jabatan : ………………………..  Asal Instansi : Dinas Pemberdayaan Perempuan Perlindungan Anak dan Keluarga Berencana (DP3AKB) Provinsi Jawa Barat  NIP : ………………………..  No HP : ………………………..  Email : ………………………..  Data lainnya : Admin Servicedesk DP3AKB |
| Mulai Tanggal dan Waktu Kejadian (*starting date and time of incident*) :  Catatan : Tuliskan sesuai waktu setempat | Tanggal 16-07-2020 |
| Bukti dari Pelapor : | Terlampir |
| Jenis Layanan/Pelaporan : | [~~Proaktif~~] [Reaktif] |
| **II. Identitas Pemilik Sistem & Laporan Insiden oleh Pemilik Sistem (\*\*)** | |
| Nama Instansi (*institution by*) : | Nama Instansi : Dinas Pemberdayaan Perempuan Perlindungan Anak dan Keluarga Berencana (DP3AKB) Provinsi Jawa Barat  Alamat Instansi : Jl. Sumatera No.50, Kota Bandung, Jawa Barat 40115, Indonesia.  Telp./Fax : (022) 4237369  Email : dp3akb@jabarprov.go.id |
| Sistem yang terkena pengaruh insiden (*systems effected due to the incident*) : | Nama Sistem : Subdomain Website Dinas Pemberdayaan Perempuan Perlindungan Anak dan Keluarga Berencana (DP3AKB) Provinsi Jawa Barat  Jenis Sistem : **~~Server~~ / Website / ~~PC~~ / ~~Network~~**  URL : **http://motekar.dp3akb.jabarprov.go.id/**  IP Address : …………..  OS : …………..  Web Server : ………….. |
| Nama Administrator / Pemilik Sistem (PIC) | <diisi oleh administrator pemilik system>  Nama : …………………….  Jabatan : …………………….  NIP : …………………….  No HP : …………………….  Email : ……………………. |
| Mulai Tanggal dan Waktu Kejadian (*starting date and time of incident*) :  Catatan : Tuliskan sesuai waktu setempat | <diisi oleh administrator pemilik system> |
| Lokasi insiden (*location of incident*) : | Hosting terdaftar pada **………………………..** |
| Deskripsi kejadian insiden (*Description of the security incident*) , disertai bukti / screenshot serangan : | \*Terlampir |
| Internet Services Provider (ISP) : | <diisi oleh administrator pemilik system>  **…………………………………..** |
| Down time or system down jika ada (system down or down time, if any) : | <diisi oleh administrator pemilik system>  [ya] [tidak]  durasi waktu : ………………………...  (\*) catatan : jika ya, tuliskan durasi waktu, selain itu abaikan |
| Tindakan teknis / kebijakan yang sudah dilakukan pertama kali: | <diisi oleh administrator pemilik system> |
| **III. Hasil Analisis dan Rekomendasi Tim Penanggulangan dan Pemulihan Insiden JabarProv-CSIRT (\*\*\*)** | |
| Kategori Insiden (*category of incident*) : | Jenis insiden :   1. web defacement 2. hacking 3. ~~malware detection~~ 4. ~~phising~~ 5. ~~spoofing~~ 6. ~~brute force~~ 7. ~~denial of service~~ 8. ~~sniffing~~   lainnya :  Berdasarkan hasil analisa dari Tim Penanggulangan dan Pemulihan Insiden JabarProv-CSIRT, bahwa insiden ini berupa serangan *defacement*, diperlukan analisa lebih lanjut terhadap sistem dengan melakukan VA ataupun *Pentest* agar mengetahui apakah terdapat kerentanan yang lainnya. |
| Sistem yang terkena pengaruh insiden (*systems effected due to the incident*) : | Nama Sistem : Website Dinas Pendidikan Provinsi Jawa Barat  Jenis Sistem : **~~Server~~ / Website / ~~PC~~ / ~~Network~~**  URL : **http://motekar.dp3akb.jabarprov.go.id/**  IP Address : 10.0.3.28 (lokal)  OS : Ubuntu  Web Server : Apache 2.4.18 |
| Lokasi insiden (*location of incident*) : | Hosting terdaftar pada **Data Center Diskominfo Provinsi Jawa Barat** |
| Internet Services Provider (ISP) : | 1. **PT Aplikanusa Lintasarta** |
| Rekomendasi Penanggulangan dan Pemulihan secara umum: | **Mitigasi :**   1. Perlu dilakukan pembangunan *website* sementara agar publikasi informasi pada *website* tetap berjalan. Atau dapat juga dilakukan pembangunan *site under maintenance*; 2. Lakukan *backup* sistem, untuk keperluan forensik ataupun untuk mengumpulkan bukti-bukti insiden; 3. Pembatasan akses terhadap sumber serangan yang ditemukan antara lain sumber *IP*, sumber *port*, serta akun user yang digunakan oleh penyerang   ***Eradication* :**   1. Lakukan hapus file *malicious*, antara lain : ***file* *defacement, file backdoor, file rootkit* ataupun *file malware;*** 2. Lakukan *uninstall* aplikasi jika ditemukan sebagai aplikasi *malicious*;   **Pemulihan :**   1. Mengaktifkan (*me-restore*) *file-file* yang telah di-*backup.* *File* dapat berupa *file* pada *web* *server*, *file* *database*. Dan gunakan aplikasi *checksum* sebagai *data* *integrity* *checker* pada *file* *backup* tersebut; 2. Lakukan *update*/*upgrade*/*patch* semua aplikasi yang digunakan pada *web* *server*. Jika menggunakan CMS, *update* versi web aplikasi, *plugins*, *themes* yang digunakan. Jika menggunakan API dapat melakukan *update* *library* yang digunakan. Selain itu perlu dilakukan update *rules* pada konfigurasi keamanan yang digunakan; 3. Lakukan *automatic updates* pada setiap aplikasi yang digunakan; 4. Lakukan pembaruan seluruh akun yang digunakan baik pada sistem operasi, web aplikasi; 5. Lakukan penerapan *secure code* pada setiap pengembangan aplikasi. |

|  |  |
| --- | --- |
| **IV. Tindakan Penanganan Insiden Lanjutan** | |
| Diisi oleh administrator website/aplikasi/system : |  |
| Diisi oleh Tim Gulih Infrastruktur Jabarprov-CSIRT : |  |
| Diisi oleh Tim Gulih Aplikasi dan Informatika Jabarprov-CSIRT : |  |
| **V. Progress Penanganan Insiden** | |
| [1] Laporan Pertama : | **Rabu, 16-07-2020** |
| [2] Analisa terhadap laporan Insiden : | **Rabu, 16-07-2020** |
| [3] Kontak Administrator Web melalui private chat dan aplikasi servicedesk : | **Rabu, 16-07-2020** |
| [4] Respon Kontak Administrator : | **Rabu, 16-07-2020** |
| [5] Pengisian Form Insiden oleh  Administrator : |  |
| [6] Rekomendasi terhadap Insiden : |  |
| [7] Penanganan Lanjutan : |  |
| [8] Eskalasi BSSN (Jika diperlukan) : |  |
| [9] Koordinasi CSIRT Eksternal (Jika  diperlukan) : |  |
| [10] Laporan Ditutup / Selesai |  |

**Keterangan :**

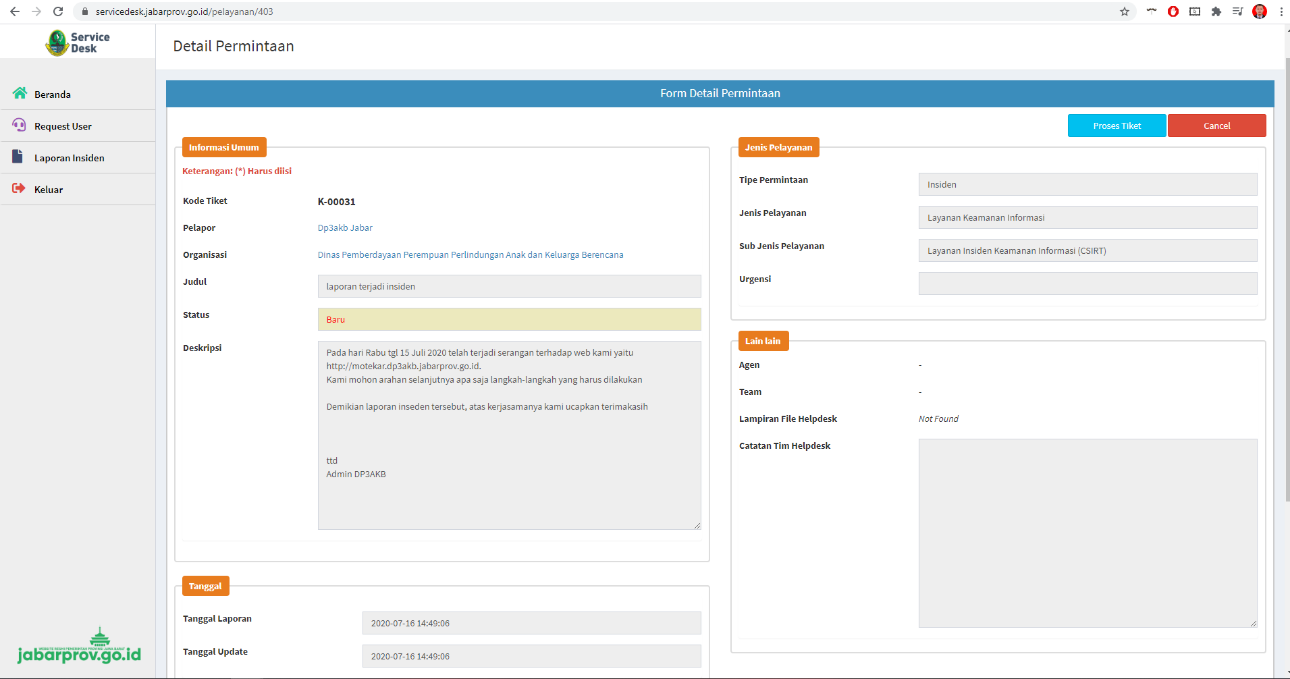
**(\*)** Diisi oleh Pelapor pertama yang melaporkan terjadinya insiden pada suatu sistem

**(\*\*)** Diisi atau dilengkapi juga oleh administrator website/aplikasi/sistem

**(\*\*\*)** Diisi oleh Tim Penanggulangan dan Pemulihan Insiden Jabarprov CSIRT

( Tim Analisis Jabarprov-CSIRT, Tim Koordinasi Jabarprov-CSIRT )

1. **LAMPIRAN PENANGANAN INCIDENT**
2. **Lampiran Pelapor**
3. Tim Jabarprov-CSIRT mendapatkan sebuah laporan yang berasal dari admin DP3AKB melalui aplikasi servicedesk bahwa website *motekar.dp3akb.jabarprov.go.id* terkena serangan *defacement* (Gambar 1).



Gambar 1. Laporan terkait website *defacement* pada website Motekar DP3AKB

1. **Lampiran Administrator Pemilik Sistem**

<diisi oleh administrator pemilik system>

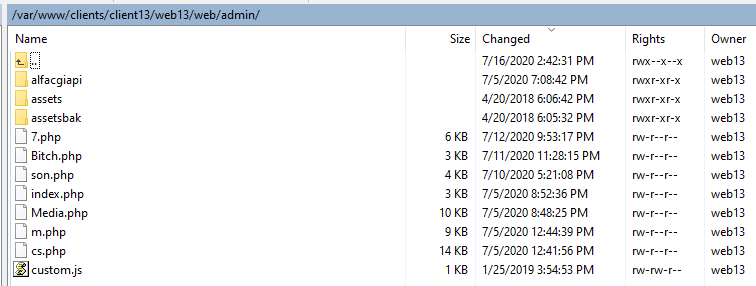
|  |  |  |
| --- | --- | --- |
| Nama | : |  |
| Jabatan | : |  |
| NIP | : |  |
| No.Hp | : |  |
| Email | : |  |

1. **Lampiran Tim Penanggulangan dan Pemulihan Insiden JabarProv-CSIRT**
2. Menindaklanjuti laporan tersebut, Tim Jabarprov-CSIRT melakukan validasi atau pengecekan ulang terhadap serangan tersebut dan ditemukan jika memang site tersebut terkena serangan *Defacement* (Gambar 2).



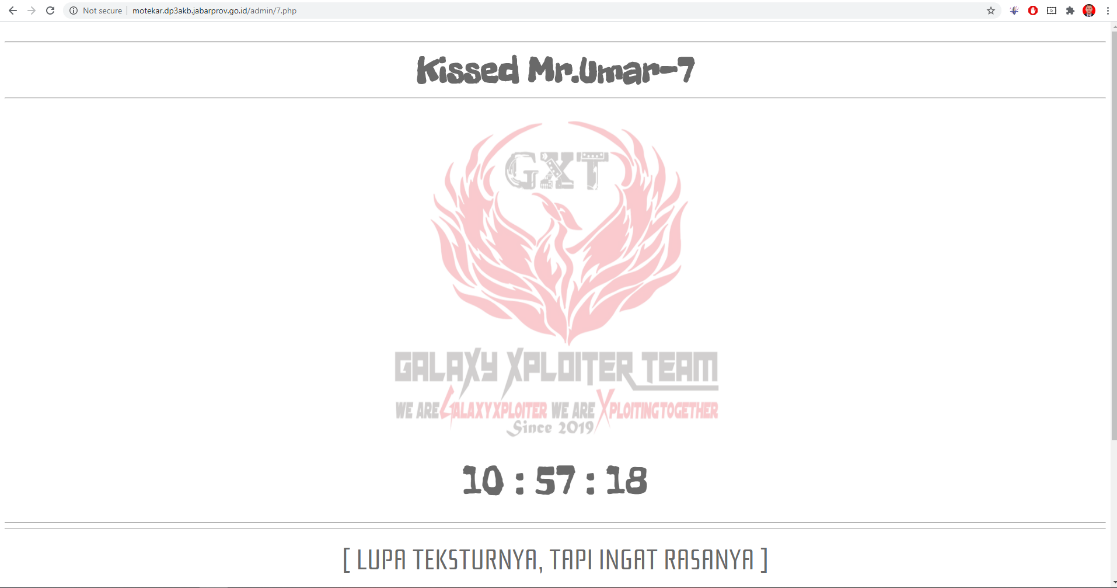
Gambar 2. Tampilan serangan *defacement* pada web *motekar.dp3akb.jabarprov.go.id*

1. Sebagai bentuk identifikasi penanganan, Tim Jabarprov-CSIRT saling melakukan koordinasi untuk penanganan yang efektif. Lalu tim Jabarprov-CSIRT melakukan pengecekan langsung terhadap *script* (menggunakan user sementara) yang digunakan pada website *motekar.dp3akb.jabarprov.go.id* dan menemukan beberapa file yang mengandung file-file sensitif hingga shell eksploit web tersebut. Antara lain:
   1. File index.php pada tiap foldernya di *replace* oleh hacker dengan file *defacement*. Hasil *defacement* tersebut dapat dilihat pada Gambar 2.
   2. Lalu saat melakukan pengecekandidapatkan beberapa file pada folder /admin, seperti ditunjukkan pada Gambar 3.

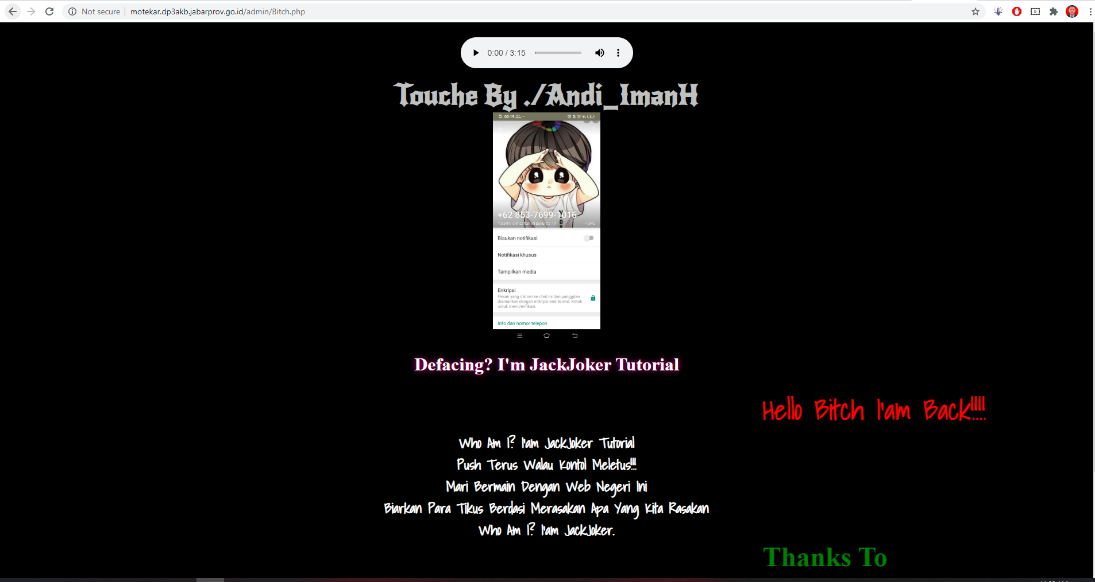


Gambar 3. File pada folder /admin.

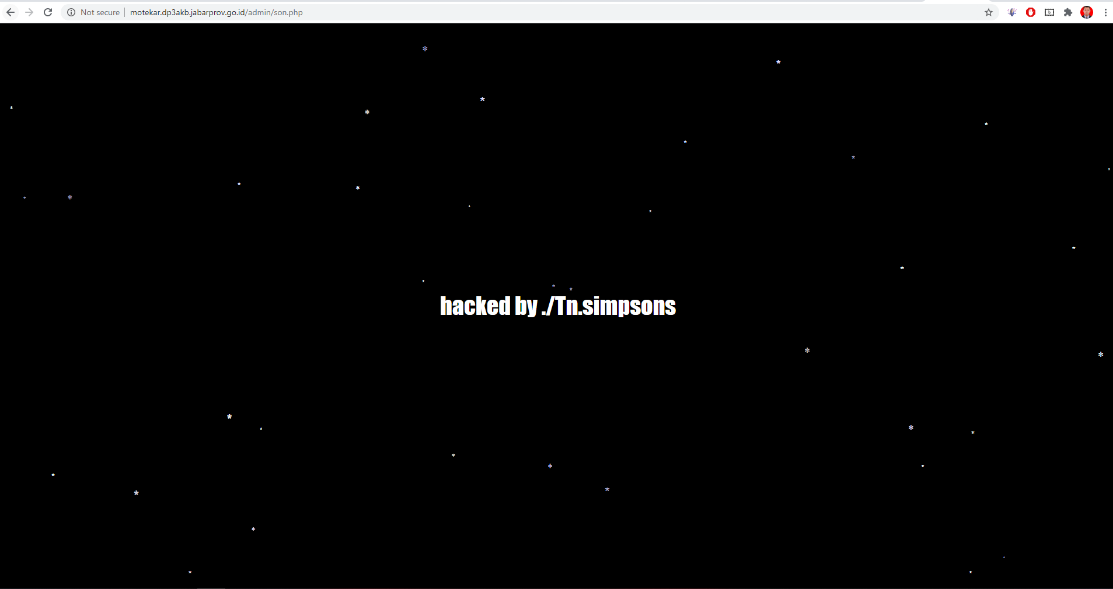
* 1. File-file pada Gambar 3 tersebut merupakan beberapa hasil serangan yang dilakukan pihak yang tidak bertanggung jawab, seperti contohnya:
     + Serangan Defacement:



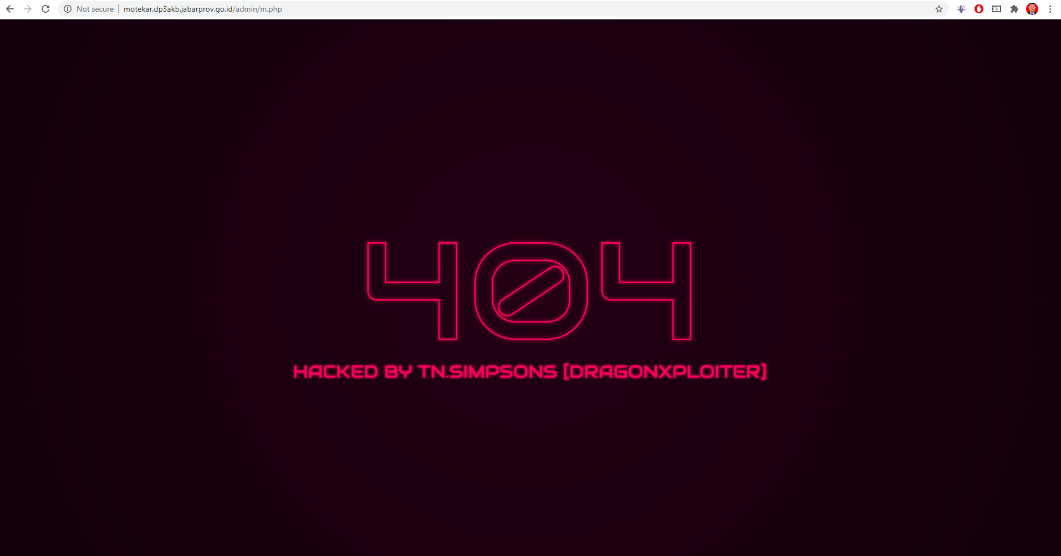
Gambar 3. Tampilan serangan *defacement* pada site /admin/7.php



Gambar 4. Tampilan serangan *defacement* pada site /admin/Bitch.php

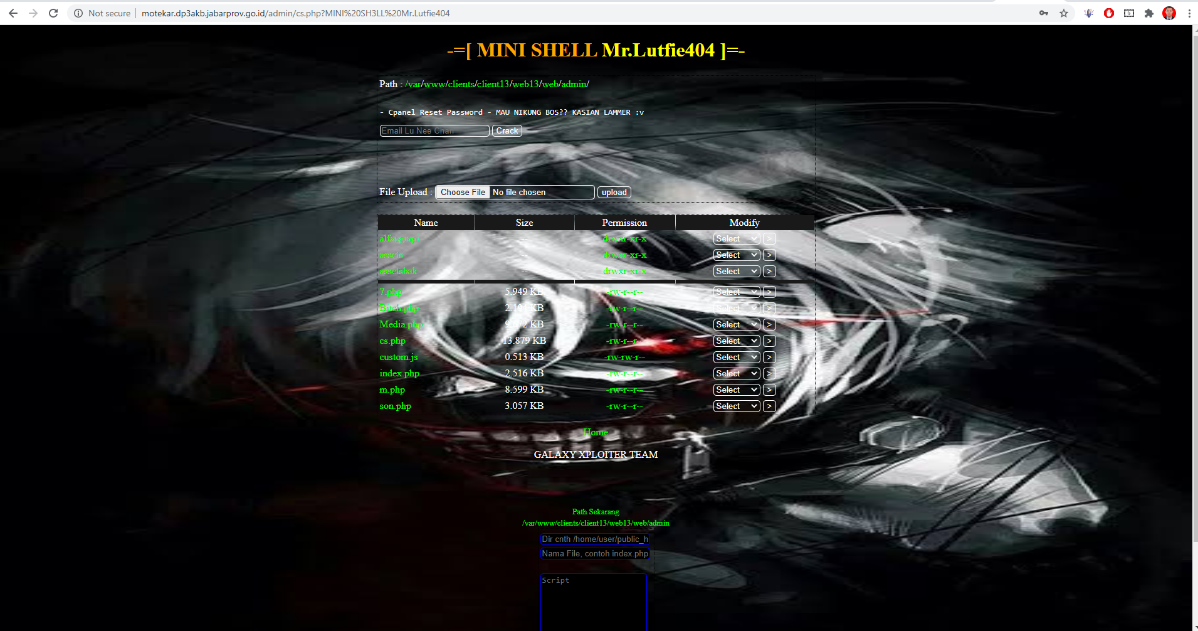


Gambar 5. Tampilan serangan *defacement* pada site /admin/son.php

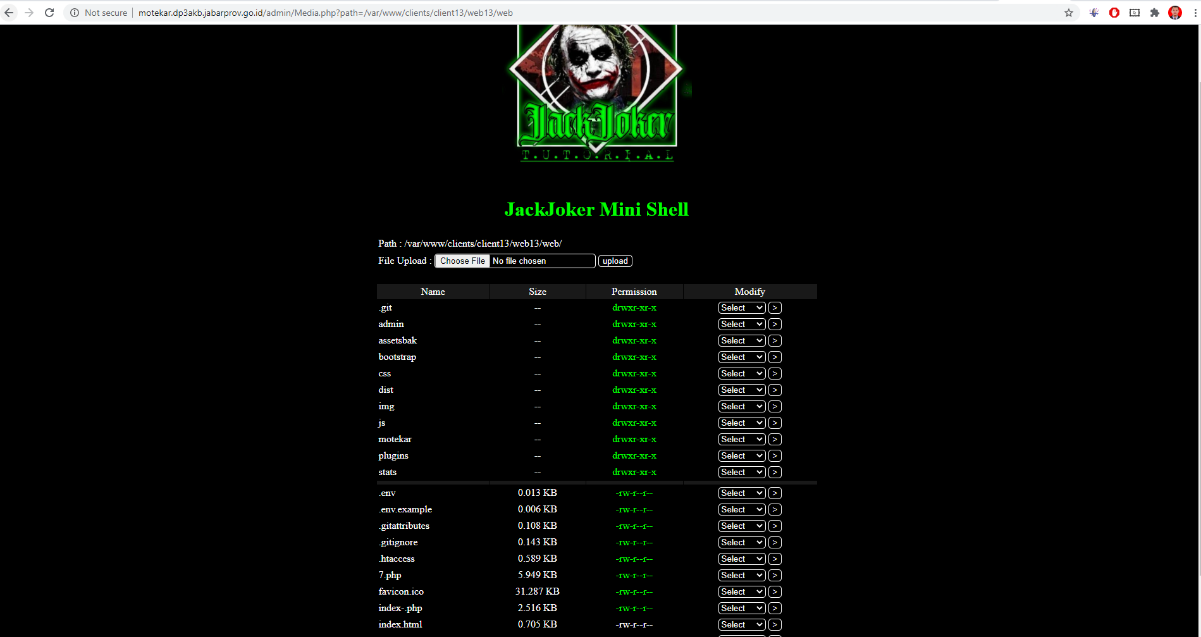


Gambar 6. Tampilan serangan *defacement* pada site /admin/m.php

* + - Terdapat beberapa, *web shell* eksploit yang digunakan pihak yang tidak bertanggung jawab untuk menyisipkan file *defacement*, antara lain:

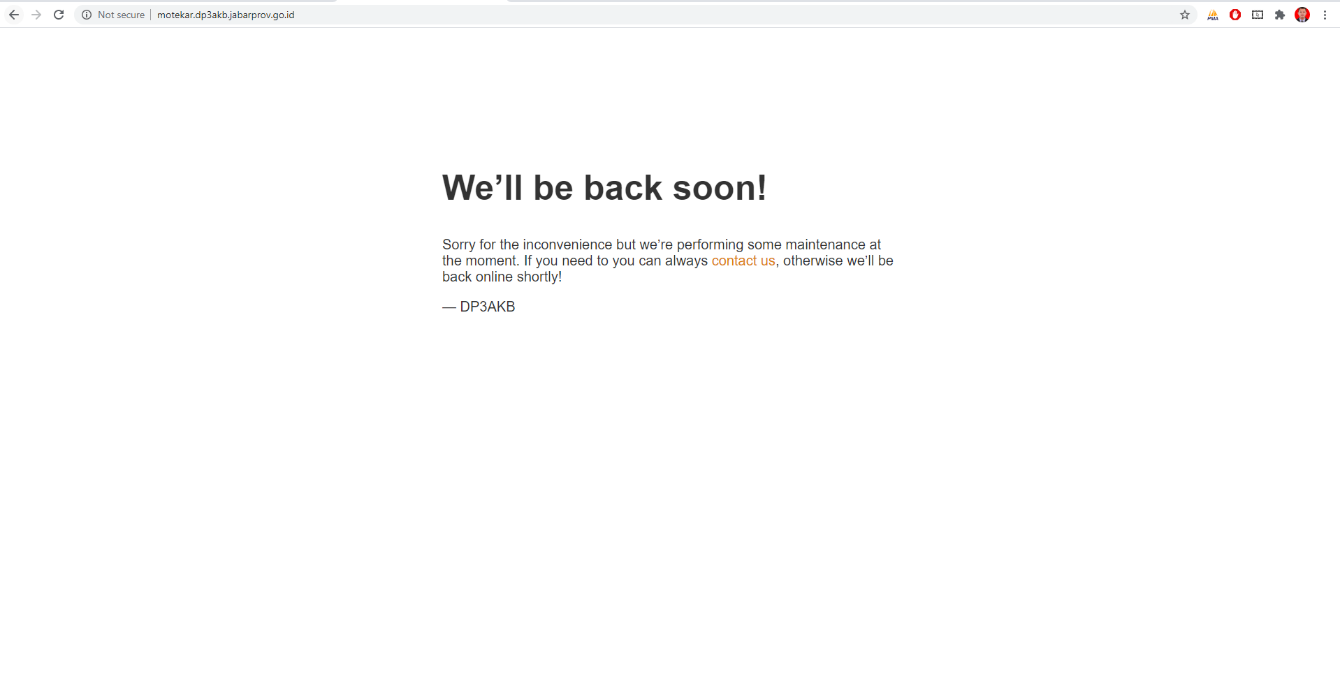


Gambar 6. Tampilan Web Shell pada site /admin/cs.php



Gambar 7. Tampilan Web Shell pada site /admin/cs.php

1. **Lampiran Tindakan Penangan Insiden Lanjutan**
2. Pada tanggal 16 Juni 2020, pengelola website motekar dp3akb merespon dengan cepat setiap laporan yang ditemukan oleh tim Jabarprov-CSIRT dan melakukan tjndakan pencegahan dengan meredirect kedalam halaman maintenance. (Gambar 8)



Gambar 8. Redirect Halaman Dissos