

Laporan IT Security Assessment

**Aplikasi Sirame
Pemerintah Kabupaten Bekasi**
<https://sirame.bekasikab.go.id/>
(Alamat IP – 103.105.197.159)

DOKUMEN v.1.0

Kode : 2023-1.0-SRM-BKS.RELEASE
Tanggal : 16 November 2023



Rilis Dokumen

Dokumen	Versi	Referensi	Author	Reviewer	Tanggal
Laporan <i>IT Security Assessment</i> Aplikasi Sirame Pemerintah Kabupaten Bekasi	1.0	2023-1.0-SRM-BKS.RELEA SE	Tim ITSA Pemerintah Kabupaten Bekasi	Ketua Tim ITSA Pemerintah Kabupaten Bekasi	16 November 2023

IT Security Assesment (ITSA)

Nama Sistem	: Aplikasi Sirame Pemerintah Kabupaten Bekasi	Tanggal Pelaksanaan :
IP Address	: 103.105.197.159	13 s.d. 16 November
Remote IP Address	: 66.96.239.91	2023
Akses	: https://sirame.bekasikab.go.id/	

Executive Summary :

1. Terdapat celah kerawanan pada Aplikasi Sirame Pemerintah Kabupaten Bekasi, yaitu Clickjacking : X-Frame-Option Header Missing, Application Support Deprecated, No Restrict on Input and Files Upload, Auto Complete Enable dan Bad Code and Implementation.
2. Secara umum Aplikasi Sirame Pemerintah Kabupaten Bekasi dikategorikan sebagai sistem aplikasi dengan tingkat **Low Risk Severity**.

Rekomendasi Perbaikan :

1. Melakukan setting keamanan header HTTP pada aplikasi.
2. Melakukan *update* pada *library* jQuery yang digunakan pada aplikasi dan/atau *dependencies* aplikasi. Namun sebelum melakukan *update library* perlu adanya pertimbangan dan pemeriksaan terhadap kompatibilitas, dimana banyak terdapat kasus *error* yang disebabkan oleh adanya ketidakcocokan *library* baru dengan *dependencies* lain pada aplikasi, sehingga perlu dilakukan *downgrade* untuk mengatasi *error* tersebut.
3. Memberikan pembatasan berupa filter dan sanitasi pada fitur input data dan *upload file*, sehingga penyerang tidak dapat mengirimkan input data dan/atau meng*upload* file berbahaya atau file dengan ukuran besar yang tidak semestinya ke aplikasi.
4. Melakukan *disable* fitur *auto-complete* pada aplikasi.
5. Menempatkan source code sesuai dengan kelas dan foldernya masing-masing, serta menghapus *link* dan/atau halaman yang tidak digunakan lagi, khususnya pada aplikasi *level production*.

Scope

Nama Sistem	: Aplikasi Sirame Pemerintah Kabupaten Bekasi
URL	: https://sirame.bekasikab.go.id/
IP Address Aplikasi	: 103.105.197.159
IP Address Pengujian	: 66.96.239.91
Tanggal Pelaksanaan	: 13 s.d. 16 November 2023

Gathering Information

1. Sistem Operasi : CentOS
2. Web Server : LiteSpeed
3. Framework : Code Igniter
4. Bahasa Pemrograman : PHP 8.1.23
5. CDN : Cloudflare
cdnjs
6. Maps : Leadflet
7. Security : reCapthca
HSTS
8. Font Script : Google Font API
Font Awesome
9. Hosting : Niagahoster
10. Performance : LazySizes
11. Java Script Framework : GSAP 3.9.1
12. Libraries : LazySizes
Isotope
Select2
OWL Carousel
Modernizr
Lodash 2.4.1
jQuery 3.4.1
DataTables 1.10.18
13. UI Framework : Bootstrap 5

14. Port Scanning :

No	Port	Protokol	State	Service	Version
1	53	-	Open	HTTP	-
2	80	-	Open	HTTPS	HTTP
3	443	-	Open	-	HTTPS
4	3128	-	Open	-	Squid-HTTP
5	8080	-	Open	-	HTTP

15. Traceroute :

```
traceroute to 103.105.197.159 (103.105.197.159), 30 hops max, 60 byte packets
. .... .
1 192.168.200.1 (192.168.200.1) 5.374 ms 4.528 ms 5.679 ms
2 192.168.200.1 (192.168.200.1) 6.057 ms !X 7.032 ms !X 6.263 ms !X
```

16. DNS Enumeration :

desa-tridayasakti.bekasikab.go.id
bekasikab.go.id
wmtv.bekasikab.go.id
sigpb.bekasikab.go.id
api-mpp.bekasikab.go.id
ns1.bekasikab.go.id
siakpus.bekasikab.go.id
opensatudata.bekasikab.go.id
ns2.bekasikab.go.id
sipemakes.bekasikab.go.id
mail.bekasikab.go.id
inlislite.bekasikab.go.id
dev-epers.bekasikab.go.id
mpp.bekasikab.go.id
ppb.bekasikab.go.id
sipd-simda.bekasikab.go.id
boss.bekasikab.go.id
ftp.bekasikab.go.id
sisling.bekasikab.go.id
socket-mpp.bekasikab.go.id
bpbd.bekasikab.go.id
vicon.bekasikab.go.id
jdih-dprd.bekasikab.go.id
cmsnewsroom.bekasikab.go.id
simpad.bekasikab.go.id
bphtb.bekasikab.go.id
hasopangan-dkp.bekasikab.go.id
sisdabima-sdabmbk.bekasikab.go.id
bisma.bekasikab.go.id
pbbm.bekasikab.go.id
siempok.bekasikab.go.id
sig-ppm.bekasikab.go.id
webr.bekasikab.go.id
kelurahan-bahagia.bekasikab.go.id
sisumaker.bekasikab.go.id
simple.bekasikab.go.id
ipad.bekasikab.go.id

pasaronline.bekasikab.go.id
bpmppt.bekasikab.go.id
tamsel.bekasikab.go.id
bpmpd.bekasikab.go.id
bplh.bekasikab.go.id
www.ciktim.bekasikab.go.id
www.bpbpd.bekasikab.go.id
dishub.bekasikab.go.id
www.dinsos.bekasikab.go.id
bkd.bekasikab.go.id
bpkpb.bekasikab.go.id
www.bojongmanggu.bekasikab.go.id
cikpus.bekasikab.go.id
www.tamara.bekasikab.go.id
tamara.bekasikab.go.id
bp4kkp.bekasikab.go.id
pmd.dpmpptsp.bekasikab.go.id
sipdah.bekasikab.go.id
bappeda.bekasikab.go.id
baghukum.bekasikab.go.id
apabae.bekasikab.go.id
www.diskominfo.bekasikab.go.id
www.bakesbangpol.bekasikab.go.id
www.bp4kkp.bekasikab.go.id
www.tambelang.bekasikab.go.id
www.bpmpppt.bekasikab.go.id
www.kukm.bekasikab.go.id
www.cibarusah.bekasikab.go.id
bakesbangpol.bekasikab.go.id
dinkes.bekasikab.go.id
disbudpora.bekasikab.go.id
www.disbudpora.bekasikab.go.id
dispar.bekasikab.go.id
satpolpp.bekasikab.go.id
cikbar.bekasikab.go.id
www.bpmpd.bekasikab.go.id
www.bkd.bekasikab.go.id
www.dinkes.bekasikab.go.id
simasb.bekasikab.go.id
www.disdamkar.bekasikab.go.id
cibirung.bekasikab.go.id

17. Penyedia Layanan *Hosting* :

NetRange:	103.0.0.0 - 103.255.255.255
CIDR:	103.0.0.0/8
NetName:	APNIC-103
NetHandle:	NET-103-0-0-0-1
Parent:	()
NetType:	Allocated to APNIC
OriginAS:	
Organization:	Asia Pacific Network Information Centre (APNIC)
RegDate:	2011-01-09
Updated:	2011-02-10
Comment:	This IP address range is not registered in the ARIN database.
Comment:	For details, refer to the APNIC Whois Database via
Comment:	WHOIS.APNIC.NET or http://wq.apnic.net/apnic-bin/whois.pl
Comment:	** IMPORTANT NOTE: APNIC is the Regional Internet Registry
Comment:	for the Asia Pacific region. APNIC does not operate networks
Comment:	using this IP address range and is not able to investigate
Comment:	spam or abuse reports relating to these addresses. For more
Comment:	help, refer to http://www.apnic.net/apnic-info/whois_search2/abuse-and-spamming
Ref:	https://rdap.arin.net/registry/ip/103.0.0.0
ResourceLink:	http://wq.apnic.net/whois-search/static/search.html
ResourceLink:	whois.apnic.net
OrgName:	Asia Pacific Network Information Centre
OrgId:	APNIC
Address:	PO Box 3646
City:	South Brisbane
StateProv:	QLD
PostalCode:	4101
Country:	AU
RegDate:	
Updated:	2012-01-24
Ref:	https://rdap.arin.net/registry/entity/APNIC
ReferralServer:	whois://whois.apnic.net
ResourceLink:	http://wq.apnic.net/whois-search/static/search.html
OrgTechHandle:	AWC12-ARIN
OrgTechName:	APNIC Whois Contact
OrgTechPhone:	+61 7 3858 3188
OrgTechEmail:	search-apnic-not-arin@apnic.net
OrgTechRef:	https://rdap.arin.net/registry/entity/AWC12-ARIN
OrgAbuseHandle:	AWC12-ARIN
OrgAbuseName:	APNIC Whois Contact
OrgAbusePhone:	+61 7 3858 3188
OrgAbuseEmail:	search-apnic-not-arin@apnic.net
OrgAbuseRef:	https://rdap.arin.net/registry/entity/AWC12-ARIN

18. Server Hosting :

http://sirame.bekasikab.go.id [302 Found] IP[103.105.197.159],
RedirectLocation[https://hotspot.maxindo.net.id/login?dst=http%3A%2F%2Fsirame.bekasikab.go.id%2F], Title[Error 302: Hotspot login required]
https://hotspot.maxindo.net.id/login?dst=http%3A%2F%2Fsirame.bekasikab.go.id%2F [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5,
IP[192.168.208.1], JQuery[2.2.3], PasswordField[password], Script, X-UA-Compatible[IE=edge]

Vulnerability Summary

No.	Jenis Vulnerability	Severity
1	<i>Clickjacking : X-Frame-Option Header Missing</i>	Medium
2	<i>Application Support Deprecated</i>	Low
3	<i>No Restrict on Input and Files Upload</i>	Low
4	<i>Auto Complete Enable</i>	Information
4	<i>Bad Code and Implementation</i>	Information

Critical Risk Findings

Tidak terdapat celah kerentanan dengan *risk severity critical*.

High Risk Findings

Tidak terdapat celah kerentanan dengan *risk severity high*.

Medium Risk Findings

1. Clickjacking : X-Frame-Option Header Missing

Deskripsi

Clickjacking merupakan celah kerentanan yang disebabkan oleh tidak dikonfigurasikannya keamanan *header* HTTP dengan baik, sehingga penyerang dapat menempatkan *frame* pada tombol atau *form input* pada aplikasi yang menjadi target serangan. Dimana apabila pengguna menekan *frame* tersebut, maka dapat mentriger instruksi yang telah ditanamkan oleh penyerang (misal mengirimkan informasi kredensial milik pengguna tanpa diketahui).

Lokasi Temuan

<https://sirame.bekasikab.go.id/>

Proof of Concept (PoC)

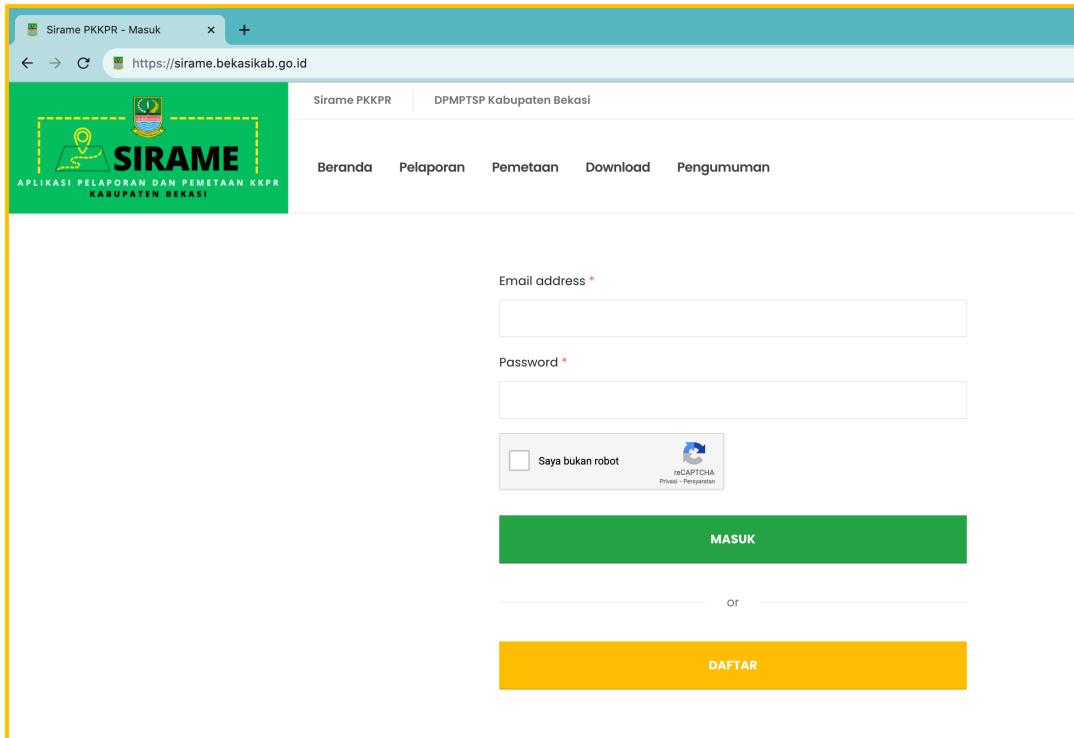
Terdapat konfigurasi keamanan *header* HTTP pada Aplikasi Sirame Bekasikab yang belum dikonfigurasi dengan baik, salah satunya adalah *X-Frame-Option*, yaitu fitur yang berfungsi untuk mencegah *web browser* untuk diembed dengan sebuah *frame* HTML. Gambar 1. dibawah menunjukkan penjelasan *X-Frame-Option*.

X-Frame-Options

[X-Frame-Options](#) tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".

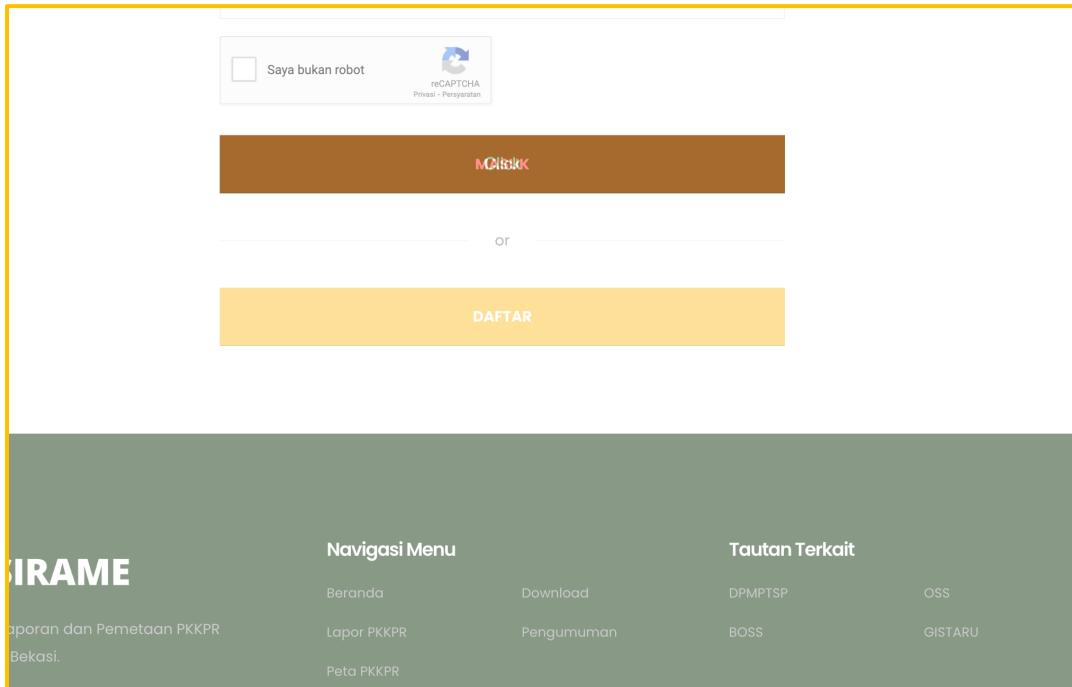
Gambar 1. Penjelasan *X-Frame-Option*.

Celah kerentanan tersebut dapat dimanfaatkan untuk melakukan serangan *clickjacking* pada aplikasi tanpa sepengetahuan / deteksi oleh pengguna. Gambar 2. menunjukkan halaman *login* pada Aplikasi Sirame Bekasikab.



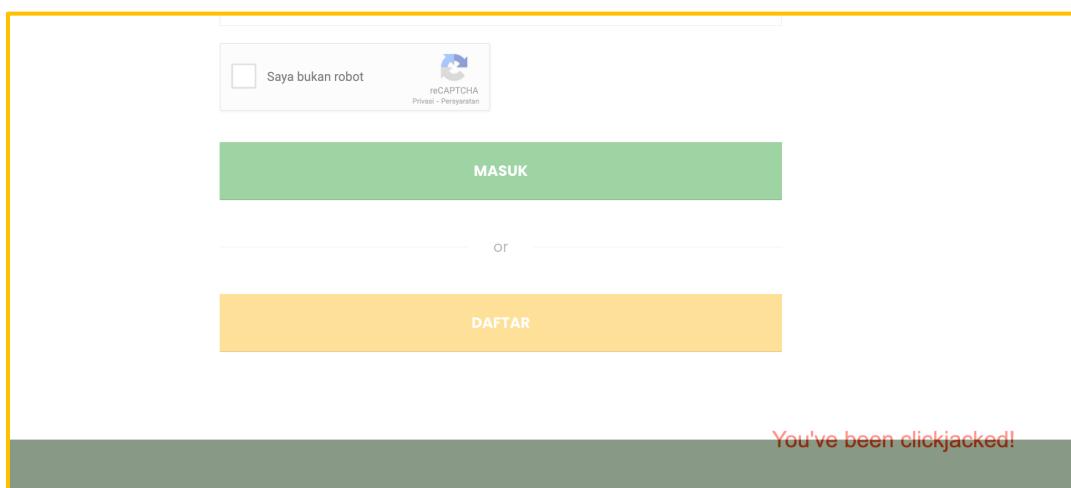
Gambar 2. Halaman *Login* pada Aplikasi Sirame Bekasikab.

Serangan *clickjacking* memiliki dampak serangan yang beragam, tergantung dari apa yang disisipkan oleh penyerang. Serangan tersebut dapat diterapkan di tombol atau *form* manapun yang diprediksi akan ditekan oleh pengguna. Kasus serangan *clickjacking* umumnya sering terjadi pada halaman *login*, dimana penyerang dapat menyisipkan pengiriman input plainteks *username* dan *password* pengguna, *ip address* pengguna atau *metadata browser* ke URL milik penyerang setiap kali pengguna menekan tombol *login*. Gambar 3. dibawah menunjukkan serangan *clickjacking* pada Aplikasi Sirame Bekasikab.



Gambar 3. Serangan *Clickjacking* pada Aplikasi Sirame Bekasikab.

Keberhasilan serangan *clickjacking* sangat tinggi, karena serangan tersebut tidak dapat dilihat secara visual oleh pengguna (dalam hal ini penyerang menggunakan *transparent frame*) dan lokasi tombolnya juga disesuaikan dengan tombol yang harus dan/atau pasti di tekan oleh pengguna. Gambar 4. dibawah menunjukkan POC serangan *clickjacking* pada Aplikasi Sirame Bekasikab.



Gambar 4. POC Serangan *Clickjacking* pada Aplikasi Sirame Bekasikab.

Berdasarkan pada hasil pemeriksaan lanjutan, selain setting X-Frame-Option, keamanan *header* HTTP Aplikasi Sirame Bekasikab juga belum mensetting beberapa parameter standar keamanan minimal pada keamanan *header* HTTP, antara lain : *Strict-Transport-Security*, *Content-Security-Policy*, *X-Content-Type-Options*, *Referrer-Policy* dan *Feature-Policy*. Gambar 5. *rating* dan penjelasan konfigurasi keamanan *header* HTTP pada Aplikasi Sirame Bekasikab.

The screenshot displays two panels from a security audit tool. The top panel, titled 'Security Report Summary', shows a large red 'F' icon indicating a failing grade. It provides basic information: Site: https://sirame.bekasikab.go.id/, IP Address: 103.105.197.159, Report Time: 10 Nov 2023 08:09:21 UTC, and Headers: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy are all marked as missing. An 'Advanced' note says 'Ouch, you should work on your security posture immediately:' followed by a 'Start Now' button. The bottom panel, titled 'Missing Headers', lists six header types with their descriptions: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy.

Gambar 5. Rating dan Penjelasan Konfigurasi Keamanan *Header* HTTP pada Aplikasi Sirame Bekasikab.

Penilaian Risiko yang diberikan berdasarkan standar OWASP versi 4 tahun 2017, adalah :

Risk Calculation		
Likelihood Factors	5.750	Medium
Impact Factors	5.375	Medium
Overall Risk Severity	5.563	Medium

Rekomendasi Perbaikan

Melakukan setting keamanan *header* HTTP pada aplikasi.

Low Risk Findings

1. Application Support Deprecated

Deskripsi

Application support deprecated merupakan celah kerentanan yang disebabkan oleh tidak diupdatenya aplikasi pendukung atau *library* yang digunakan pada *dependencies* aplikasi, sehingga memungkinkan penyerang untuk melakukan eksploitasi melalui celah kerentanan pada aplikasi pendukung atau *library* tersebut.

Lokasi Temuan

<https://sirame.bekasikab.go.id/>

Proof of Concept (PoC)

Terdapat beberapa aplikasi pendukung atau *library* pada Aplikasi Sirame Bekasikab yang belum diupdate, antara lain *library* jQuery. jQuery merupakan *library open source* yang berfungsi sebagai kumpulan fungsi *JavaScript* siap pakai untuk memudahkan *programmer* dalam melakukan *koding*. jQuery dapat berjalan dengan stabil (kompatibel) pada banyak *web browser* dan merupakan *library* yang paling banyak digunakan oleh *programmer* dalam mengembangkan aplikasi. Gambar 6. menunjukkan celah kerentanan *library* jQuery pada Aplikasi Sirame Bekasikab.

CVE-2019-11358 Detail

Current Description
jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native Object.prototype.

[— Hide Analysis Description](#)

Analysis Description
jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native Object.prototype.

Severity	CVSS Version 3.x	CVSS Version 2.0
CVSS 3.x Severity and Metrics:		
NVD	NIST: NVD	Base Score: 6.1 MEDIUM
		Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Gambar 6. Celah Kerentanan *Library* jQuery pada Aplikasi Sirame Bekasikab.

Berdasarkan pada informasi celah kerentanan tersebut diketahui bahwa pada *library* jQuery dibawah versi 3.6.x memiliki celah kerentanan *object prototype pollution* pada *jQuery.extend*, dimana jika terdapat sebuah input pada aplikasi yang tidak di filter dengan baik, maka memungkinkan penyerang untuk dapat memperpanjang *object prototype* asli. Selain itu jQuery dibawah versi 3.6.x juga dilaporkan memiliki permasalahan terhadap parsing HMTL. Gambar 7. menunjukkan *low level attack* pada aspek kerahasiaan dan integritas data berdasarkan penilaian CVSS versi 3.0 untuk *library* jQuery pada Aplikasi Sirame Bekasikab.

CVSS v3.1 Severity and Metrics:	
Base Score:	6.1 MEDIUM
Vector:	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
Impact Score:	2.7
Exploitability Score:	2.8
<hr/>	
Attack Vector (AV):	Network
Attack Complexity (AC):	Low
Privileges Required (PR):	None
User Interaction (UI):	Required
Scope (S):	Changed
Confidentiality (C):	Low
Integrity (I):	Low
Availability (A):	None

Gambar 7. Penilaian CVSS Versi 3.0 untuk *Library* jQuery pada Aplikasi Sirame Bekasikab.

Penilaian Risiko yang diberikan berdasarkan standar OWASP versi 4 tahun 2017, adalah :

Risk Calculation		
Likelihood Factors	2.625	Low
Impact Factors	3.375	Medium
Overall Risk Severity	3.000	Low

Rekomendasi Perbaikan

Melakukan *update* pada *library* jQuery yang digunakan pada aplikasi dan/atau *dependencies* aplikasi. Namun sebelum melakukan *update* *library* perlu adanya

pertimbangan dan pemeriksaan terhadap kompatibilitas, dimana banyak terdapat kasus *error* yang disebabkan oleh adanya ketidakcocokan *library* baru dengan *dependencies* lain pada aplikasi, sehingga perlu dilakukan *downgrade* untuk mengatasi *error* tersebut. Gambar 8. menunjukkan kasus *error* karena *update library* jQuery.

I had to move from 3.5 back to 3.4.1 because my Bootstrap 4 navbar would not work. I am using Rails 6, Ruby 2.7.1. Is this an issue you will be fixing soon? Interested because I'm getting a notice of a security vulnerability in 3.4.1.

Thank you.

Gambar 8. Kasus *Error* Karena *Update Library* jQuery.

2. **No Restrict on Input and Files Upload**

Deskripsi

No Restrict on Input and Files Upload merupakan celah kerentanan yang disebabkan oleh tidak dilakukannya pembatasan berupa filter dan sanitasi pada fitur input dan/atau fitur *upload* file, sehingga memungkinkan penyerang untuk mengirimkan input data dan/atau mengupload file berbahaya atau file dengan ukuran besar yang tidak semestinya dalam rangka mengangu layanan atau fitur tertentu sampai dengan *take over* aplikasi.

Lokasi Temuan

<https://sirame.bekasikab.go.id/kkpr/form-add>

Proof of Concept (PoC)

Penguji mencoba melakukan pengisian / input data pelaku usaha dan persetujuan PKKPR dengan menggunakan random input dan beberapa sintaks serangan. Gambar 9. menunjukkan input data pada Aplikasi Sirame Bekasikab.

SIRAME PKKPR

PKKPR Sirame PKKPR

Data Pelaku Usaha

Nama Pelaku Usaha: a NPWP: 1

Alamat Kantor: b

Telepon Kantor: c Email Kantor: d@email.com

Status Penanaman Modal: e

Skala Usaha: f Luas Tanah yang Dimohon: 1

Alamat Lokasi Usaha: g

Kecamatan Lokasi Usaha: Cabangbungin Kelurahan Lokasi Usaha: Jayalaksana

Data Persetujuan PKKPR

Nomor PKKPR: 1

Luas Tanah yang disetujui: 1 Peruntukan Pemanfaatan Ruang: h

Gambar 9. Input Data pada Aplikasi Sirame Bekasikab.

Berdasarkan pada hasil observasi, diketahui bahwa seluruh input yang diberikan oleh pengujji diterima dan disimpan kedalam database Aplikasi Sirame Bekasikab. Gambar 10. menunjukkan penyimpanan data pada Aplikasi Sirame Bekasikab.

SIRAME PKKPR

PKKPR Sirame PKKPR

*Data pelaporan PKKPR tidak dapat diubah atau dihapus apabila sudah berstatus "KELENGKAPAN DITERIMA".

Berhasil!
Simpan data berhasil: silakan upload kelengkapan untuk tahapan berikutnya.

Show: 10 entries	#	Nomor	Status	Terbit	Pelaku Usaha	Telepon	KBBI	Pemanfaatan R
	1	(select extractvalue)	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	2	(select load_file)	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	3	(select*from(select	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	4	1	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	5	1 and (select*from(s	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	6	1 and 2317=02317--	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	7	1 and 4063=40630--	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	8	1 and 4609=46090	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	9	1 and 5105=5105--	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h
	10	1 and 5282=5274--	BELUM UPLOAD KELENGKAPAN	01/11/2023	a	c	i	h

Gambar 10. Penyimpanan Data pada Aplikasi Sirame Bekasikab.

Celah kerentanan ini terlihat sederhana, namun jika dapat dimanfaatkan oleh penyerang, maka dapat menyebabkan dampak yang sangat fatal, antara lain : ganguan layanan pada aplikasi (*down*), ganguan manajemen data (*database penuh*), *take over server*, sampai dengan penanaman *backdoor* pada aplikasi. Penilaian Risiko yang diberikan berdasarkan standar OWASP versi 4 tahun 2017, adalah :

Risk Calculation		
Likelihood Factors	2.500	Low
Impact Factors	4.575	Medium
Overall Risk Severity	3.538	Low

Rekomendasi Perbaikan

Memberikan pembatasan berupa filter dan sanitasi pada fitur input data dan *upload file*, sehingga penyerang tidak dapat mengirimkan input data dan/atau mengupload file berbahaya atau file dengan ukuran besar yang tidak semestinya ke aplikasi.

Information Risk Findings

1. Auto Complete Enable

Deskripsi

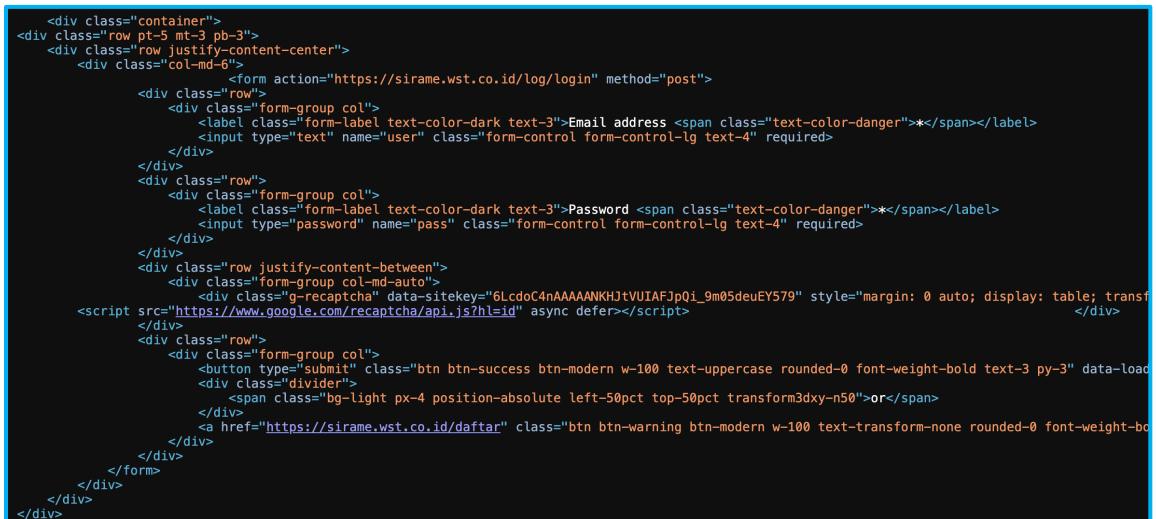
Auto complete enable merupakan celah kerentanan yang disebabkan oleh tidak disettingnya fitur *auto complete* pada form *input* pengguna, sehingga mengizinkan *web browser* untuk menyimpan *cache* input yang diberikan oleh pengguna yang dapat dimanfaatkan oleh penyerang untuk mengenerate inputan milik pengguna.

Lokasi Temuan

<https://sirame.bekasikab.go.id/>

Proof of Concept (PoC)

Implementasi *auto complete fill* pada dasarnya merupakan fitur *support* untuk kemudahan bagi pengguna, akan tetapi berdasarkan konsep keamanan sistem informasi, fitur tersebut tidak disarankan untuk digunakan, karena dapat dimanfaatkan oleh pihak yang tidak berkepentingan untuk melakukan pencurian sampai dengan *take over* akun milik pengguna. Gambar 11. menunjukkan *auto-complete enabled* pada Aplikasi Sirame Bekasikab.



```
<div class="container">
<div class="row pt-5 mt-3 pb-3">
    <div class="row justify-content-center">
        <div class="col-md-6">
            <form action="https://sirame.wst.co.id/log/login" method="post">
                <div class="row">
                    <div class="form-group col">
                        <label class="form-label text-color-dark text-3">Email address <span class="text-color-danger">*</span></label>
                        <input type="text" name="user" class="form-control form-control-lg text-4" required>
                    </div>
                </div>
                <div class="row">
                    <div class="form-group col">
                        <label class="form-label text-color-dark text-3">Password <span class="text-color-danger">*</span></label>
                        <input type="password" name="pass" class="form-control form-control-lg text-4" required>
                    </div>
                </div>
                <div class="row justify-content-between">
                    <div class="form-group col-md-auto">
                        <div class="g-recaptcha" data-sitekey="6Lcd0C4nAAAAAKHJtVUIAFJpQi_9m05deuEY579" style="margin: 0 auto; display: table; transform: rotate(-90deg);>
                            <script src="https://www.google.com/recaptcha/api.js?hl=id" async defer></script>
                        </div>
                    </div>
                    <div class="row">
                        <div class="form-group col">
                            <button type="submit" class="btn btn-success btn-modern w-100 text-uppercase rounded-0 font-weight-bold text-3 py-3" data-load="true">
                                <div class="divider">
                                    <span class="bg-light px-4 position-absolute left-50px top-50px transform3dxy-n50">or</span>
                                </div>
                                <a href="https://sirame.wst.co.id/daftar" class="btn btn-warning btn-modern w-100 text-transform-none rounded-0 font-weight-bo
                            </div>
                        </div>
                    </div>
                </div>
            </form>
        </div>
    </div>
</div>
```

Gambar 11. *Auto-Complete Enabled* pada Aplikasi Sirame Bekasikab.

Penilaian Risiko yang diberikan berdasarkan standar OWASP versi 4 tahun 2017, adalah :

Risk Calculation		
Likelihood Factors	2.750	Low
Impact Factors	1.500	Low
Overall Risk Severity	2.125	Information

Rekomendasi Perbaikan

Melakukan *disable* fitur *auto-complete* pada aplikasi.

2. Bad Code and Implementation

Deskripsi

Bad code and implementation merupakan celah kerentanan yang disebabkan oleh adanya kesalahan dalam melakukan koding terhadap aplikasi secara sebagian dan/atau keseluruhan, sehingga menyebabkan kegagalan pada fitur atau tampil data yang tidak sesuai untuk dapat di eksploitasi oleh penyerang.

Lokasi Temuan

- <https://sirame.bekasikab.go.id/>
- <https://sirame.bekasikab.go.id/.profile>
- <https://sirame.bekasikab.go.id/application>
- <https://sirame.bekasikab.go.id/@>

Proof of Concept (PoC)

Terdapat kekurangan dari hasil pemrograman pada Aplikasi Sirame Bekasikab, namun kekurangan tersebut tidak bersifat kritis dan mempengaruhi kinerja sistem informasi secara umum. Antara lain : pemrograman yang kurang rapih, karena adanya *source code* yang digunakan untuk mengkonfigurasi tampilan *front end* tidak pada kelasnya dan adanya fitur tidak terpakai yang dikomen (dalam hal ini tidak dihapus) pada level production. Gambar 12. menunjukkan *bad code and implementation* pada Aplikasi Sirame Bekasikab.

```

<div class="owl-carousel owl-theme nav-style-1 nav-arrows-thin nav-font-size-lg nav-outside mb-0" data-plugin-options=">
<div>
    <div class="testimonial testimonial-style-5 px-lg-5 mx-lg-5">
        <blockquote>
            <p class="mb-0 line-height-8 font-weight-medium text-4">SIRAME PKKPR merupakan aplikasi yang menyediakan layanan
            </blockquote>
            <div class="testimonial-author border-0">
                <><strong class="font-weight-extra-bold pt-2">SIRAME PKKPR</strong><span>DPMPPTSP - KABUPATEN BEKASI</span></p>
            </div>
        </div>
    </div>
<div>

-gradient m-0">
=container py-2">
lass="row align-items-center text-center text-lg-start py-5">
iv class="col-lg-9 mb-3 mb-lg-0">
<p class="text-color-light text-4-5 font-weight-medium line-height-4 mb-0">
    <span class="d-inline-block appear-animation" data-appear-animation="fadeInUpShorterPlus" data-appear-animation=">
        <strong>Pelaporan PKKPR</strong> - Silakan daftar akun untuk melakukan pelaporan PKKPR
    </span>
</p>
div>
iv class="col-lg-3 pt-3 pt-lg-0 text-center text-lg-end">
    <span class="d-inline-block appear-animation" data-appear-animation="fadeInUpShorterPlus" data-appear-animation=">
        <a href="https://sirame.wst.co.id/daftar" class="btn btn-light text-color-tertiary border-0 text-3-5 font-we">
    </span>
div>

="border-0 custom-bg-color-grey-1" style="margin-bottom: -50px">
=container py-5">

<!--<div class="anim-hover-translate-top-10px transition-3ms">
    <div class="card">
        <div class="card-body p-5">
            <div class="d-flex flex-row">
                <div class="pt-2">
                    
                <div class="pt-4">
                    <h4 class="mb-2 text-5 font-weight-semi-bold">Warehousing</h4>
                    <p class="mb-2 font-weight-medium text-3">Lorem ipsum dolor sit amet, conse ctetur adipisci scing elit.</p>
                    <a href="#" class="text-uppercase text-2-5 stretched-link text-decoration-underline text-color-primary text-color-hover-tertiary font-weight-semi-bold transition-3ms">
                </div>
            </div>
        </div>
    </div>
<div class="anim-hover-translate-top-10px transition-3ms">
    <div class="card">
        <div class="card-body p-5">
            <div class="d-flex flex-row">
                <div class="pt-2">
                    
                <div class="pt-4">
                    <h4 class="mb-2 text-5 font-weight-semi-bold">Air Freight</h4>
                    <p class="mb-2 font-weight-medium text-3">Lorem ipsum dolor sit amet, conse ctetur adipisci scing elit.</p>
                    <a href="#" class="text-uppercase text-2-5 stretched-link text-decoration-underline text-color-primary text-color-hover-tertiary font-weight-semi-bold transition-3ms">
                </div>
            </div>
        </div>
    </div>
<div class="anim-hover-translate-top-10px transition-3ms">
    <div class="card">
        <div class="card-body p-5">
            <div class="d-flex flex-row">
                <div class="pt-2">
                    
                <div class="pt-4">
                    <h4 class="mb-2 text-5 font-weight-semi-bold">Ground Shipping</h4>
                    <p class="mb-2 font-weight-medium text-3">Lorem ipsum dolor sit amet, conse ctetur adipisci scing elit.</p>
                    <a href="#" class="text-uppercase text-2-5 stretched-link text-decoration-underline text-color-primary text-color-hover-tertiary font-weight-semi-bold transition-3ms">
                </div>
            </div>
        </div>
    </div>
</div-->

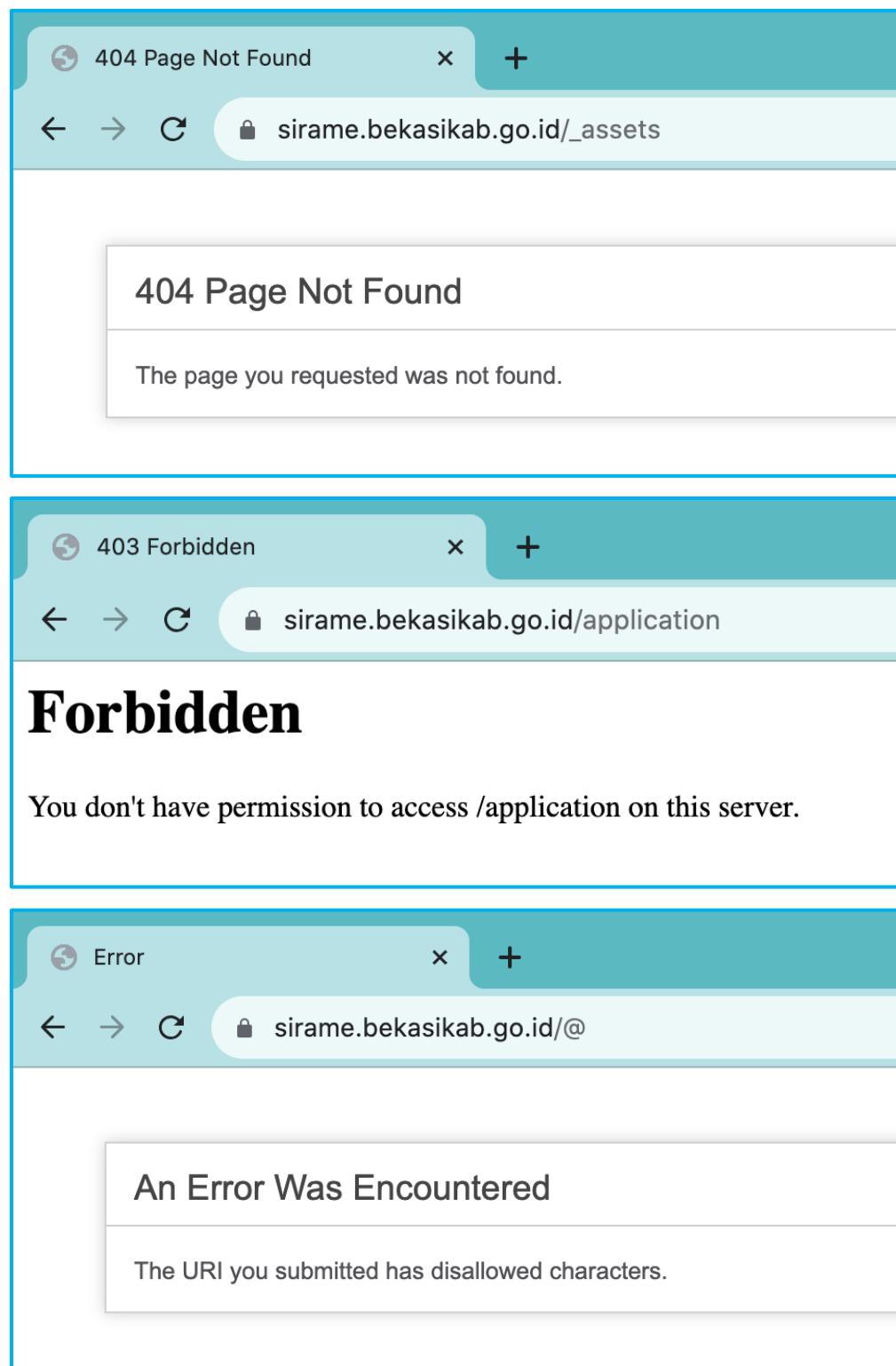
<div class="ms-auto d-none d-lg-inline-block">
    <!--<ul class="nav nav-pills">
        <li class="nav-item dropdown">
            <a class="nav-link text-2 p-0 text-color-default" href="#" role="button" id="dropdownLanguage">
                english
                <i class="fas fa-angle-down"></i>
            </a>
            <div class="dropdown-menu dropdown-menu-end text-2" aria-labelledby="dropdownLanguage">
                <a class="dropdown-item text-color-default" href="#">English</a>
                <a class="dropdown-item text-color-default" href="#">Español</a>
                <a class="dropdown-item text-color-default" href="#">Française</a>
            </div>
        </li>
    </ul>-->
</div>

```

Gambar 12. Bad Code and Implementation pada Aplikasi Sirame Bekasikab.

Selain itu pengujian juga dilakukan dengan mencoba akses terhadap beberapa halaman pada Aplikasi Sirame Bekasikab, jika terdapat rekues ke halaman yang *forbidden* (403), tidak ada (404), *internal server error* (500) dan/atau *error* lainnya, maka Aplikasi Sirame Bekasikab akan melemparkan *handling* secara

default dari *framework*, sehingga memberikan informasi kepada penyerang terkait aplikasi *web server* yang digunakan. Gambar 13. menunjukkan *error page* pada Aplikasi Sirame Bekasikab.



Gambar 13. *Error Page* pada Aplikasi Sirame Bekasikab.

Berdasarkan standar penilaian OWASP versi 4 tahun 2017, temuan ini dapat dinilai sebagai berikut :

Risk Calculation		
Likelihood Factors	2.375	Low
Impact Factors	1.375	Low
Overall Risk Severity	1.875	Information

Rekomendasi Perbaikan

Menempatkan source code sesuai dengan kelas dan foldernya masing-masing, serta menghapus *link* dan/atau halaman yang tidak digunakan lagi, khususnya pada aplikasi *level production*.