MİLLİ
KİBERTƏHLÜKƏSİZLİK
AGENTLİYİ

MİLLİ
KİBERTƏHLÜKƏSİZLİK
AGENTLİYİ

KONFİDENSİAL

# Statik tətbiq təhlükəsizliyi və proqram asılılıqlarının təhlili üzrə
# SAST / SCA HESABATI

# Razılaşma

| Audit aparan tərəf | Milli Kibertəhlükəsizlik Agentliyi |
|---|---|
| Audit olunan təşkilat / layihələr | MKA, NCERT (CERT Backend), PDP Backend və CERTKIDS |
| Yoxlama növü | SAST — Statik tətbiq təhlükəsizliyi testi; SCA — Proqram tərkibinin və asılılıqların təhlili |

## Məxfilik bəyanatı

Təqdim edilən hesabat konfidensial və mülkiyyət hüququnu əks etdirən texniki məlumatları ehtiva edir. Hesabatın tam və ya qismən paylaşılması, kopyalanması və üçüncü tərəfə ötürülməsi yalnız Milli Kibertəhlükəsizlik Agentliyinin razılığı ilə mümkündür.

Hesabat istifadəçi tərəfindən təqdim edilmiş SAST və SCA skan nəticələri əsasında hazırlanmışdır. Dinamik istismar, penetrasiya testi və istehsal mühitində əl ilə təsdiqləmə bu işin həcminə daxil deyil. Buna görə tapıntıların real istismar oluna bilməsi tətbiqin konfiqurasiyası, giriş nəzarətləri, versiya aralıqları və işə salınma mühitindən asılı olaraq ayrıca yoxlanılmalıdır.

## Terminlər və layihələrin adlandırılması

| Qısaltma | Açıqlama |
|---|---|
| **MKA** | Milli Kibertəhlükəsizlik Agentliyi |
| **NCERT** | National Computer Emergency Response Team; hesabatda CERT Backend layihəsi ilə əlaqələndirilir. |
| **PDP** | Personal Data Protection; PDP Backend layihəsi |
| **CERTKIDS** | CERT-in uşaqlar üçün nəzərdə tutulmuş hissəsi |
| **SAST** | Mənbə kodunda zəifliklərin statik üsulla aşkarlanması |
| **SCA** | Üçüncü tərəf paketlərinin, versiyaların və məlum təhlükəsizlik advisory-lərinin təhlili |

# İşin həcmi

Yoxlama dörd proqram layihəsi üzrə təqdim edilmiş statik analiz və proqram asılılığı nəticələrini əhatə edir:

1. CERTKIDS — tətbiq mənbə kodu və Composer asılılıqları;
2. PDP Backend — tətbiq mənbə kodu və Composer asılılıqları;
3. CERT Backend / NCERT — tətbiq mənbə kodu və Composer asılılıqları;
4. MKA — Composer asılılıqları. MKA layihəsi üzrə təqdim olunan məlumatlarda ayrıca SAST tapıntısı göstərilməyib.

## Metodologiya

SAST mərhələsində mənbə kodunda hardcoded secrets, giriş məlumatlarının yoxlanılması, fayl yükləmə siyasəti və çıxış kontekstinə uyğun sanitizasiya kimi təhlükəsizlik nəzarətləri qiymətləndirilmişdir. Tapıntılar CWE və OWASP Top 10:2021 kateqoriyaları ilə uyğunlaşdırılmışdır.

SCA mərhələsində composer.json və composer.lock fayllarındakı paketlər, versiyalar, GHSA və CVE identifikatorları əsasında təhlil edilmişdir. Təqdim edilmiş nəticələrdə düzəldilmiş konkret versiya göstərilmədiyi hallarda, hesabat versiya nömrəsi uydurmur və rəsmi advisory-də göstərilən patched release-ə yüksəltməyi tələb edir.

1. Aktivlərin və manifestlərin müəyyən edilməsi;
2. SAST tapıntılarının təsnifatı və manual review ehtiyacının qeyd edilməsi;
3. SCA advisory-lərinin layihə və paket versiyaları ilə xəritələndirilməsi;
4. Risklərin prioritetləşdirilməsi;
5. Remediation və re-test meyarlarının hazırlanması.

## Risk səviyyəsinin qiymətləndirilməsi

| Ciddilik | CVSS v3 aralığı | Tərif |
|---|---|---|
| **Kritik** | 9.0–10.0 | Məxfi məlumatların və ya yüksək səlahiyyətli etimadnamələrin ələ keçirilməsi, sistem səviyyəli komprometasiya və ya geniş təsir ehtimalı. Dərhal tədbir tələb olunur. |
| **Yüksək** | 7.0–8.9 | Məlumat sızması, stored XSS, icazəsiz əməliyyat, təhlükəli fayl yükləmə və ya geniş istifadə olunan asılılıq zəifliyi. Qısa müddətdə aradan qaldırılmalıdır. |
| **Orta** | 4.0–6.9 | İstismar əlavə şərtlər və ya məhdud giriş tələb edir. Planlı remediation tələb olunur. |
| **Aşağı** | 0.1–3.9 | Birbaşa istismar ehtimalı məhduddur, lakin müdafiə dərinliyini zəiflədir. |

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# İcraçı xülasəsi

Təqdim edilmiş məlumatlar əsasında 5 SAST tapıntısı müəyyən edilmişdir: 2 kritik hardcoded private key, 2 yüksək riskli məhdudlaşdırılmamış fayl yükləmə konfiqurasiyası və 1 yüksək riskli HTML atribut kontekstində yanlış sanitizasiya. SCA nəticələri dörd layihədə 24 asılılıq qeydini və 28 yüksək riskli advisory occurrence-nı əhatə edir.

## Tapıntıların bölgüsü

| 2 | 10 | 0 | 0 |
|---|---|---|---|
| **Kritik** | **Yüksək** | **Orta** | **Aşağı** |

## Layihələr üzrə nəticələr

| Layihə | SAST | SCA paket qeydi | SCA advisory occurrence | Əsas risk |
|---|---|---|---|---|
| CERTKIDS | 3: 2 Kritik, 1 Yüksək | 6 | 7 Yüksək | Service-account private key-lərin repository-də saxlanması |
| PDP Backend | 1 Yüksək | 6 | 7 Yüksək | Fayl yükləmə MIME allow-list çatışmazlığı və vulnerable dependencies |
| CERT Backend / NCERT | 1 Yüksək | 6 | 7 Yüksək | HTML atributunda kontekstə uyğun olmayan sanitizasiya |
| MKA | Ayrıca tapıntı təqdim edilməyib | 6 | 7 Yüksək | Vulnerable Composer dependencies |

## Prioritet tədbirlər

1. CERTKIDS repository-də aşkarlanmış hər iki Google service-account private key dərhal deaktiv və ya revoke edilməli, yeni açarlar yaradılmalı və bütün istifadə nöqtələri təhlükəsiz secret manager-ə keçirilməlidir.
2. Açarların Git tarixçəsindən silinməsi üçün repository history rewrite aparılmalı; yalnız cari faylı silməklə kifayətlənilməməlidir.
3. Dörd layihədə Composer asılılıqları rəsmi GHSA/CVE advisory-lərində göstərilən patched versiyalara yüksəldilməli və composer.lock yenilənməlidir.
4. Filament FileUpload komponentlərində MIME və extension allow-list tətbiq edilməli, SVG yalnız təhlükəsiz sanitizasiya və ayrıca servis vasitəsilə qəbul edilməlidir.
5. CERT Backend Blade şablonunda alt atributu üçün {!! !!} çıxışı dayandırılmalı və Blade-in atribut-kontekstli escape mexanizmindən istifadə edilməlidir.

## Tapıntıların ümumi siyahısı

| ID | Layihə | Ciddilik | Tapıntı |
|---|---|---|---|
| SAST-01 | CERTKIDS | Kritik | Hardcoded Private Key — public credentials file |
| SAST-02 | CERTKIDS | Kritik | Hardcoded Private Key — analytics credentials file |
| SAST-03 | CERTKIDS | Yüksək | File Upload Without a MIME Allow-List |
| SAST-04 | PDP Backend | Yüksək | File Upload Without a MIME Allow-List |
| SAST-05 | CERT Backend | Yüksək | HTML atributunda yanlış sanitizer konteksti |
| SCA-01 | 4 layihə | Yüksək | Guzzle CookieJar — dot-only cookie domain |
| SCA-02 | 4 layihə | Yüksək | Guzzle HTTPS proxy downgrade və credential leakage |
| SCA-03 | 4 layihə | Yüksək | Filament unauthenticated temporary file upload |
| SCA-04 | 4 layihə | Yüksək | Filament Forms RichEditor stored XSS |
| SCA-05 | 4 layihə | Yüksək | Filament Tables relationship scope bypass |
| SCA-06 | 4 layihə | Yüksək | Guzzle PSR-7 CR/LF header injection |
| SCA-07 | 4 layihə | Yüksək | Laravel temporary signed URL expiration bypass |

# SAST — Texniki tapıntılar

Bu bölmədə mənbə kodu üzrə təqdim edilmiş beş tapıntı ətraflı təsvir olunur. Private key materialı hesabatda təhlükəsizlik məqsədilə redaktə edilmişdir; tam etimadnamə təkrar göstərilmir.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SAST-01 — Repository-də hardcoded Google Service Account private key

| Kritik | Secrets | CWE-798 | OWASP A07:2021 | FP ehtimalı: 15% |
|---|---|---|---|---|

| Layihə | CERTKIDS |
|---|---|
| Mənbə kodu / manifest | certkids/public/service-acount-certkids-local.json:5 |
| Status | Confirmed; unauthenticated; partial evidence; manual review tələb olunur |

## Tapıntının təsviri

public/ qovluğu daxilində Google service-account credentials JSON faylında PEM formatlı private key saxlanılır. Faylın adı və yerləşməsi credential materialının tətbiq artefaktı və ya web-accessible qovluq ilə birlikdə yayılma riskini artırır. Private key-in mənbə koduna commit edilməsi etimadnamənin repository klonları, backup-lar, CI artefaktları və loglar vasitəsilə yayılmasına səbəb ola bilər.

## Potensial təsir

Açar aktivdirsə, hücumçu service account-un IAM səlahiyyətləri çərçivəsində Google Cloud resurslarına giriş əldə edə, məlumat oxuya və ya dəyişə, servis adından API çağırışları edə bilər. public/ altında yerləşmə əlavə olaraq birbaşa web exposure ehtimalı yaradır. Açarın sadəcə fayldan silinməsi əvvəlki Git commit-lərindəki sızmanı aradan qaldırmır.

## Təqdim edilmiş sübut

```
"type": "service_account",
"project_id": "atmia-1710233715554",
"private_key_id": "5e3ee4d728da0ec319a70c1402692d547f6808be",
"private_key": "-----BEGIN PRIVATE KEY-----\n[REDACTED]\n-----END PRIVATE KEY-----",
"client_email": "certkids@atmia-1710233715554.iam.gserviceaccount.com"
```

## Tövsiyə olunan düzəlişlər

- Mövcud private key dərhal revoke/deaktiv edilməli və kompрometasiya olunmuş hesab edilməlidir.
- Yeni credential yaradılmalı, tətbiq secret manager, workload identity və ya environment-based credential mexanizminə keçirilməlidir.
- Fayl public/ və repository-dən silinməli; Git tarixçəsi filter-repo/BFG kimi idarə olunan proseslə təmizlənməlidir.
- Service account IAM rolları least privilege prinsipi ilə yenidən qiymətləndirilməlidir.
- Google Cloud audit log-ları private_key_id və service account üzrə şübhəli istifadə üçün araşdırılmalıdır.
- CI/CD prosesinə secret scanning və commit blocking əlavə edilməlidir.

## Yenidən yoxlama meyarları

- Köhnə açarın deaktiv və ya silinmiş olduğu idarəetmə panelində təsdiqlənir.
- Repository cari ağacında və bütün əlçatan Git tarixçəsində PEM markerləri tapılmır.
- Tətbiq yeni secret-management mexanizmi ilə funksional testləri keçir.
- Secret scanner təkrar işə salındıqda tapıntı bağlanır.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SAST-02 — Analytics qovluğunda hardcoded Google Service Account private key

| Kritik | Secrets | CWE-798 | OWASP A07:2021 | FP ehtimalı: 15% |
|---|---|---|---|---|

| Layihə | CERTKIDS |
|---|---|
| Mənbə kodu / manifest | certkids/storage/analytics/service-account-credentials.json:5 |
| Status | Confirmed; unauthenticated; partial evidence; manual review tələb olunur |

## Tapıntının təsviri

storage/analytics qovluğunda saxlanılan credentials JSON faylında ikinci Google service-account PEM private key-i mövcuddur. storage qovluğu web server konfiqurasiyasından asılı olaraq birbaşa açıq olmaya bilər, lakin credential-ın repository-də saxlanması özlüyündə real hardcoded secret zəifliyidir.

## Potensial təsir

Açar aktivdirsə, voice-assistant-432110 layihəsində saffman service account-un səlahiyyətləri sui-istifadə edilə bilər. Repository-yə, deployment artefaktlarına və backup-lara çıxışı olan şəxslər credential-dan kənar sistemdən istifadə edə bilər. Səlahiyyətlər genişdirsə, nəticə məlumat sızması, resurs dəyişiklikləri və maliyyə itkisi ola bilər.

## Təqdim edilmiş sübut


```
"type": "service_account",
"project_id": "voice-assistant-432110",
"private_key_id": "3d6436544c7aa432012a405df1b3617a00724fdc",
"private_key": "-----BEGIN PRIVATE KEY-----\n[REDACTED]\n-----END PRIVATE KEY-----",
"client_email": "saffman@voice-assistant-432110.iam.gserviceaccount.com"
```


## Tövsiyə olunan düzəlişlər

- Private key dərhal revoke edilməli və yeni açar yalnız təhlükəsiz secret storage vasitəsilə tətbiqə təqdim edilməlidir.
- Repository və Git tarixçəsi credential faylından təmizlənməlidir.
- storage/analytics və deployment konfiqurasiyası web-accessibility baxımından yoxlanılmalıdır.
- Service account rolları və audit log-ları araşdırılmalı, artıq səlahiyyətlər çıxarılmalıdır.
- Credential faylları .gitignore və CI policy ilə bloklanmalıdır.

## Yenidən yoxlama meyarları

- Köhnə private_key_id artıq aktiv deyil.
- Git tarixçəsində private key və credential JSON izləri yoxdur.
- Tətbiq yeni credential mexanizmi ilə işləyir və least privilege testləri uğurludur.
- SAST/secret scan nəticəsi təkrar yoxlamada bağlanır.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SAST-03 — Şəkil yükləməsində MIME allow-list-in açıq göstərilməməsi

| Yüksək | Validation | CWE-434 | OWASP A04:2021 | FP ehtimalı: 40% |
|---|---|---|---|---|

| Layihə | CERTKIDS |
|---|---|
| Mənbə kodu / manifest | certkids/app/Filament/Fabricator/PageBlocks/PageHead.php:19 |
| Status | Confirmed pattern; partial evidence; Filament versiyası və runtime config manual yoxlanmalıdır |

## Tapıntının təsviri

Filament FileUpload komponentində ->image() istifadə edilir, lakin acceptedFileTypes və ya sərt MIME allow-list açıq şəkildə təyin edilmir. Konfiqurasiyadan və istifadə olunan Filament versiyasından asılı olaraq image/* SVG fayllarını da qəbul edə bilər. Sanitizasiya və təhlükəsiz serving mexanizmi yoxdursa, SVG daxilində aktiv kontent stored XSS riskinə çevrilə bilər.

## Potensial təsir

Zərərli fayl qəbul edilərək eyni origin-dən inline və ya uyğun Content-Type ilə təqdim olunarsa, admin və ya istifadəçi brauzerində script icrası, session məlumatlarının oğurlanması və admin əməliyyatlarının sui-istifadəsi mümkün ola bilər. Admin-scoped komponent olması ehtimalı istismar əlçatanlığını azaldır, lakin təsiri aradan qaldırmır.

## Təqdim edilmiş sübut

```
FileUpload::make('image')
    ->label('Şəkil Üst')
    ->image()
    ->directory('page-head')
// acceptedFileTypes([...]) göstərilməyib
```

## Tövsiyə olunan düzəlişlər

- acceptedFileTypes(['image/jpeg', 'image/png', 'image/webp']) kimi sərt allow-list tətbiq edilməlidir.
- SVG biznes tələbi deyilsə tam bloklanmalıdır. Tələbdirsə ayrıca sanitizer, rasterization və təhlükəsiz content-disposition siyasəti tətbiq edilməlidir.
- Server tərəfdə MIME magic-byte yoxlaması aparılmalı; yalnız client extension-a etibar edilməməlidir.
- Fayl adları server tərəfindən yaradılmalı, storage public execution-dan ayrılmalı və maksimum ölçü limiti müəyyən edilməlidir.
- Yüklənmiş fayllar X-Content-Type-Options: nosniff və uyğun Content-Disposition ilə təqdim edilməlidir.

## Yenidən yoxlama meyarları

- SVG, HTML və polyglot test faylları rədd edilir.
- JPEG/PNG/WebP kimi icazəli formatlar magic-byte və MIME yoxlamasından keçir.
- Yüklənmiş fayl birbaşa açıldıqda script icrası baş vermir.
- SAST qaydası acceptedFileTypes konfiqurasiyasını görərək bağlanır və manual test təsdiqlənir.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SAST-04 — PDP Backend şəkil yükləməsində MIME allow-list-in açıq göstərilməməsi

| Yüksək | Validation | CWE-434 | OWASP A04:2021 | FP ehtimalı: 40% |
|---|---|---|---|---|

| Layihə | PDP Backend |
|---|---|
| Mənbə kodu / manifest | pdp-backend/app/Filament/Resources/HuquqMovzuResource.php:61 |
| Status | Confirmed pattern; partial evidence; runtime configuration manual yoxlanmalıdır |

## Tapıntının təsviri

HuquqMovzuResource daxilində image_1 sahəsi ->image() ilə konfiqurasiya olunub, lakin qəbul edilən MIME tipləri ayrıca allow-list ilə məhdudlaşdırılmayıb. Filament konfiqurasiyası image/* qəbul etdikdə SVG və digər riskli formatlar qəbul oluna bilər.

## Potensial təsir

Yükləmə sahəsinə çıxışı olan istifadəçi zərərli aktiv kontent yerləşdirə bilər. Fayl frontend və ya admin panelində təhlükəsiz sanitizasiya olmadan render edilərsə stored XSS, content spoofing və zərərli faylın etibarlı domen üzərindən paylanması riski yaranır.

## Təqdim edilmiş sübut

```
FileUpload::make('image_1')
    ->label('Şəkil 1')
    ->image()
    ->directory('huquq-movzulari')
// explicit MIME allow-list göstərilməyib
```

## Tövsiyə olunan düzəlişlər

- acceptedFileTypes(['image/jpeg', 'image/png', 'image/webp']) tətbiq edilməlidir.
- SVG qəbul ediləcəksə sanitizer və təhlükəsiz rasterization prosesi tətbiq edilməlidir; əks halda bloklanmalıdır.
- Fayl məzmunu server-side MIME və magic-byte əsasında yoxlanılmalıdır.
- Upload authorization, rate limit, ölçü limiti və antivirus/malware scanning nəzərdən keçirilməlidir.
- Public storage-da script execution mümkün olmamalıdır.

## Yenidən yoxlama meyarları

- Riskli MIME və extension kombinasiyaları rədd edilir.
- İcazəli şəkillər problemsiz yüklənir və təhlükəsiz response header-ları ilə göstərilir.
- SVG stored XSS test payload-u icra olunmur.
- SAST və manual re-test tapıntının aradan qalxdığını təsdiqləyir.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SAST-05 — HTML atributunda element-kontekst sanitizer istifadəsi

| Yüksək | XSS | CWE-79 | OWASP A03:2021 | FP ehtimalı: 55% |
|---|---|---|---|---|

| Layihə | CERT Backend / NCERT |
|---|---|
| Mənbə kodu / manifest | cert-backend/resources/views/front/pages/hesabatlar.blade.php:282 |
| Status | Context mismatch confirmed; exploitability title mənbəyi və Purifier profili ilə manual yoxlanmalıdır |

## Tapıntının təsviri

Blade şablonunda report title Purifier::clean ilə emal edilir, lakin nəticə alt atributunun daxilində {!! !!} vasitəsilə raw output kimi yazılır. HTMLPurifier əsasən HTML element kontekstinə uyğun sanitizasiya edir; atribut dəyəri üçün lazım olan quote və attribute-context escaping-i təmin edən mexanizmlə eyni deyil.

## Potensial təsir

Təcavüzkar report title sahəsini idarə edə bilirsə və purifier profili təhlükəli quote və attribute sərhədlərini tam neytrallaşdırmırsa, img elementinə yeni atribut əlavə etmək və event handler vasitəsilə stored XSS yaratmaq mümkün ola bilər. İstismar uğurlu olduqda istifadəçi sessiyası və admin əməliyyatları riskə düşür.

## Təqdim edilmiş sübut

```
<img ...
  src="{{ asset('assets/front/images/hesabatlar/card.svg') }}"
  alt="{!! Purifier::clean($report->title[app()->getLocale()]
      ?? $report->title['az'] ?? '') !!}">
// Raw output attribute context daxilində istifadə olunur
```

## Tövsiyə olunan düzəlişlər

- alt atributunda raw {!! !!} çıxışı dayandırılmalı və {{ ... }} ilə Blade escaping istifadə edilməlidir.
- Title plain text kimi saxlanmalı; HTML tələb olunmayan sahədə Purifier::clean əvəzinə mətn normalizasiyası tətbiq edilməlidir.
- Atribut dəyəri üçün framework-in kontekstə uyğun escaping mexanizmi istifadə edilməlidir.
- Mövcud title məlumatları təhlükəli payload-lar üçün audit edilməli və lazım gəldikdə təmizlənməlidir.
- CSP, HttpOnly/SameSite cookie və input authorization əlavə müdafiə qatları kimi tətbiq edilməlidir.

## Yenidən yoxlama meyarları

- Quote, angle bracket və event-handler payload-ları alt atributundan çıxa bilmir.
- Render olunmuş HTML-də istifadəçi dəyəri entity-escaped görünür.
- Brauzer və avtomatlaşdırılmış XSS testində script icrası baş vermir.
- SAST context-mismatch qaydası təkrar skanda bağlanır.

# SCA — Asılılıqların təhlili

Dörd layihədə eyni yeddi advisory ailəsi müşahidə olunur. Paket versiyaları layihələr arasında fərqli olsa da, təqdim edilmiş skan nəticələri hər birini yüksək riskli kimi işarələyir. Düzəliş zamanı composer.json constraint-ləri və composer.lock-da faktiki quraşdırılmış versiya birlikdə yoxlanılmalıdır.

## Layihə və versiya matrisi

| Paket | PDP Backend | MKA | CERT Backend | CERTKIDS |
|---|---|---|---|---|
| guzzlehttp/guzzle | 7.11.1 | 7.10.0 | 7.11.0 | 7.10.0 |
| filament/filament | ^3.3 | ^3.3 | ^3.3 | ^3.3 |
| filament/forms | v3.3.50 | v3.3.49 | v3.3.49 | v3.3.47 |
| filament/tables | v3.3.50 | v3.3.49 | v3.3.49 | v3.3.47 |
| guzzlehttp/psr7 | 2.11.0 | 2.9.0 | 2.11.0 | 2.8.0 |
| laravel/framework | ^12.0 | ^12.0 | ^12.0 | ^12.0 |

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SCA-01 — Guzzle CookieJar-da yalnız nöqtədən ibarət domain-in bütün hostlarla uyğunlaşması

| Yüksək | Dependency | CWE-1395 | OWASP A06:2021 | FP ehtimalı: layihəyə görə 10–40% |
|---|---|---|---|---|

| Paket | guzzlehttp/guzzle |
|---|---|
| Advisory | GHSA-cwxw-98qj-8qjx / CVE-2026-55767 |
| Təsir olunan layihələr | PDP Backend, MKA, CERT Backend / NCERT, CERTKIDS |

## Tapıntının təsviri

guzzlehttp/guzzle CookieJar domen uyğunlaşdırmasında yalnız nöqtədən ibarət cookie domain dəyərini düzgün məhdudlaşdırmır və nəticədə cookie müxtəlif hostlara uyğun hesab edilə bilər. Təqdim edilmiş skan bütün dörd layihədəki Guzzle versiyalarını təsirlənmiş kimi göstərir.

## Potensial təsir

Tətbiq etibarsız və ya xarici mənbədən cookie qəbul edirsə, cookie isolation pozula və session/authentication məlumatları nəzərdə tutulmayan hostlara göndərilə bilər. Real risk tətbiqin CookieJar istifadəsindən və daxil olan cookie-lərin mənbəyindən asılıdır.

## Layihələr üzrə sübut

| Layihə | Təqdim edilmiş versiya | Manifest | FP |
|---|---|---|---|
| PDP Backend | guzzle 7.11.1; forms/tables 3.3.50; psr7 2.11.0 | pdp-backend/composer.lock və composer.json | 15% |
| MKA | guzzle 7.10.0; forms/tables 3.3.49; psr7 2.9.0 | etx/composer.lock və composer.json | 15% |
| CERT Backend / NCERT | guzzle 7.11.0; forms/tables 3.3.49; psr7 2.11.0 | cert-backend/composer.lock və composer.json | 35% |
| CERTKIDS | guzzle 7.10.0; forms/tables 3.3.47; psr7 2.8.0 | certkids/composer.lock və composer.json | 10% |

## Tövsiyə olunan düzəlişlər

- guzzlehttp/guzzle rəsmi advisory-də göstərilən patched versiyaya yüksəldilməlidir.
- composer.lock yenilənməli və bütün dörd layihədə eyni təhlükəsiz minimum versiya siyasəti tətbiq edilməlidir.
- CookieJar istifadə nöqtələri və untrusted cookie ingestion manual audit edilməlidir.
- Dependency pinning və composer audit CI pipeline-da məcburi edilməlidir.

## Yenidən yoxlama meyarları

- composer show guzzlehttp/guzzle patched versiyanı göstərir.
- composer audit GHSA-cwxw-98qj-8qjx tapıntısını qaytarmır.
- Dot-only domain test case-i cookie-ni digər hostlara göndərmir.
- Regression və inteqrasiya testləri uğurludur.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SCA-02 — HTTPS proxy əlaqəsinin cleartext-ə səssiz endirilməsi

| Yüksək | Dependency | CWE-1395 | OWASP A06:2021 | FP ehtimalı: layihəyə görə 10–40% |
|---|---|---|---|---|

| Paket | guzzlehttp/guzzle |
|---|---|
| Advisory | GHSA-wpwq-4j6v-78m3 / CVE-2026-55568 |
| Təsir olunan layihələr | PDP Backend, MKA, CERT Backend / NCERT, CERTKIDS |

## Tapıntının təsviri

Təqdim edilmiş advisory-yə əsasən Guzzle müəyyən HTTPS proxy ssenarisində əlaqəni cleartext-ə endirə və proxy credential-larını şifrələnməmiş formada ötürə bilər. Dörd layihənin Guzzle versiyaları skan tərəfindən təsirlənmiş kimi qeyd olunub.

## Potensial təsir

Tətbiq authenticated HTTPS proxy istifadə edirsə, şəbəkəni müşahidə edən hücumçu proxy istifadəçi adı və parolunu ələ keçirə bilər. Sonrakı mərhələdə proxy infrastrukturuna icazəsiz giriş, trafik müşahidəsi və daxili resurslara çıxış mümkün ola bilər.

## Layihələr üzrə sübut

| Layihə | Təqdim edilmiş versiya | Manifest | FP |
|---|---|---|---|
| PDP Backend | guzzle 7.11.1; forms/tables 3.3.50; psr7 2.11.0 | pdp-backend/composer.lock və composer.json | 15% |
| MKA | guzzle 7.10.0; forms/tables 3.3.49; psr7 2.9.0 | etx/composer.lock və composer.json | 15% |
| CERT Backend / NCERT | guzzle 7.11.0; forms/tables 3.3.49; psr7 2.11.0 | cert-backend/composer.lock və composer.json | 35% |
| CERTKIDS | guzzle 7.10.0; forms/tables 3.3.47; psr7 2.8.0 | certkids/composer.lock və composer.json | 40% |

## Tövsiyə olunan düzəlişlər

- Guzzle advisory-də göstərilən patched release-ə yüksəldilməlidir.
- Proxy konfiqurasiyasında TLS məcbur edilməli və downgrade hallarına fail-closed yanaşması tətbiq edilməlidir.
- Mövcud proxy credential-ları risk qiymətləndirilməsindən sonra rotasiya edilməlidir.
- Şəbəkə log-larında cleartext proxy authentication izləri araşdırılmalıdır.

## Yenidən yoxlama meyarları

- composer audit advisory-ni göstərmir.
- HTTPS proxy testində TLS saxlanılır və downgrade baş vermir.
- Proxy credential-ları packet capture-da açıq görünmür.
- Tətbiqin outbound HTTP funksiyaları regression testdən keçir.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SCA-03 — Filament authentication səhifələrində unauthenticated temporary file upload

| Yüksək | Dependency | CWE-1395 | OWASP A06:2021 | FP ehtimalı: layihəyə görə 10–40% |
|---|---|---|---|---|

| Paket | filament/filament |
|---|---|
| Advisory | GHSA-44wp-g8f4-f4v5 / CVE-2026-48500 |
| Təsir olunan layihələr | PDP Backend, MKA, CERT Backend / NCERT, CERTKIDS |

## Tapıntının təsviri

filament/filament paketində authentication səhifələrində autentifikasiya olunmamış temporary file upload imkanı barədə yüksək riskli advisory mövcuddur. Bütün layihələr composer.json daxilində ^3.3 constraint-i istifadə edir; faktiki resolved versiya composer.lock ilə təsdiqlənməlidir.

## Potensial təsir

İstismar olunan konfiqurasiyada hücumçu autentifikasiyasız müvəqqəti fayl yükləyə, storage resurslarını tükədə, zərərli faylları sistemə yerləşdirə və digər upload zəifliklərı ilə birləşdirərək daha ciddi təsir yarada bilər.

## Layihələr üzrə sübut

| Layihə | Təqdim edilmiş versiya | Manifest | FP |
|---|---|---|---|
| PDP Backend | guzzle 7.11.1; forms/tables 3.3.50; psr7 2.11.0 | pdp-backend/composer.lock və composer.json | 20% |
| MKA | guzzle 7.10.0; forms/tables 3.3.49; psr7 2.9.0 | etx/composer.lock və composer.json | 20% |
| CERT Backend / NCERT | guzzle 7.11.0; forms/tables 3.3.49; psr7 2.11.0 | cert-backend/composer.lock və composer.json | 40% |
| CERTKIDS | guzzle 7.10.0; forms/tables 3.3.47; psr7 2.8.0 | certkids/composer.lock və composer.json | 20% |

## Tövsiyə olunan düzəlişlər

- filament/filament rəsmi advisory-də göstərilən fixed versiyaya yüksəldilməli və composer.lock yenilənməlidir.
- Authentication səhifələrində upload komponentləri və Livewire temporary upload endpoint-ləri inventarlaşdırılmalıdır.
- Unauthenticated upload endpoint-lərinə rate limit, file size limit və MIME allow-list tətbiq edilməlidir.
- Temporary storage periodik təmizlənməli və public execution-dan ayrılmalıdır.

## Yenidən yoxlama meyarları

- Faktiki Filament versiyası patched range-dədir.
- Autentifikasiyasız temporary upload cəhdi 401/403 və ya təhlükəsiz rejection ilə nəticələnir.
- composer audit GHSA-44wp-g8f4-f4v5 tapıntısını qaytarmır.
- Login və digər auth flow-lar regression testdən keçir.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SCA-04 — Disabled RichEditor-də sanitizasiya olunmamış HTML render edilməsi

| Yüksək | Dependency | CWE-1395 | OWASP A06:2021 | FP ehtimalı: layihəyə görə 10–40% |
|---|---|---|---|---|

| Paket | filament/forms |
|---|---|
| Advisory | GHSA-m9cv-24rx-8mv7 / CVE-2026-55409 |
| Təsir olunan layihələr | PDP Backend, MKA, CERT Backend / NCERT, CERTKIDS |

## Tapıntının təsviri

filament/forms paketinin təqdim edilmiş versiyalarında disabled RichEditor sahəsinin sanitizasiya olunmamış HTML render etməsi barədə stored XSS advisory-si mövcuddur. PDP Backend 3.3.50, MKA və CERT Backend 3.3.49, CERTKIDS 3.3.47 istifadə edir.

## Potensial təsir

Hücumçu RichEditor məzmununu əvvəlcədən daxil edə bilirsə, disabled/read-only görünüşə baxan səlahiyyətli istifadəçinin brauzerində script icra edilə bilər. Bu, session hijacking, admin action və məlumat sızmasına səbəb ola bilər.

## Layihələr üzrə sübut

| Layihə | Təqdim edilmiş versiya | Manifest | FP |
|---|---|---|---|
| PDP Backend | guzzle 7.11.1; forms/tables 3.3.50; psr7 2.11.0 | pdp-backend/composer.lock və composer.json | 15% |
| MKA | guzzle 7.10.0; forms/tables 3.3.49; psr7 2.9.0 | etx/composer.lock və composer.json | 15% |
| CERT Backend / NCERT | guzzle 7.11.0; forms/tables 3.3.49; psr7 2.11.0 | cert-backend/composer.lock və composer.json | 35% |
| CERTKIDS | guzzle 7.10.0; forms/tables 3.3.47; psr7 2.8.0 | certkids/composer.lock və composer.json | 10% |

## Tövsiyə olunan düzəlişlər

- filament/forms vulnerable range-dən yuxarı patched versiyaya yüksəldilməlidir.
- RichEditor məzmunu save və render mərhələsində təhlükəsiz HTML allow-list ilə sanitizasiya edilməlidir.
- Disabled/read-only komponentlərin raw HTML render etmədiyi təsdiqlənməlidir.
- CSP tətbiq edilərək inline script icrası əlavə olaraq məhdudlaşdırılmalıdır.

## Yenidən yoxlama meyarları

- composer audit GHSA-m9cv-24rx-8mv7 tapıntısını qaytarmır.
- Stored XSS test payload-u disabled RichEditor görünüşündə icra olunmur.
- Təhlükəsiz formatlaşdırma funksiyaları saxlanılır.
- Bütün admin panel formaları regression testdən keçir.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SCA-05 — Attach/Associate əməliyyatlarında relationship scope-un tətbiq edilməməsi

| Yüksək | Dependency | CWE-1395 | OWASP A06:2021 | FP ehtimalı: layihəyə görə 10–40% |
|---|---|---|---|---|

| Paket | filament/tables |
|---|---|
| Advisory | GHSA-7q3w-xqjw-g3cr / CVE-2026-48067 |
| Təsir olunan layihələr | PDP Backend, MKA, CERT Backend / NCERT, CERTKIDS |

## Tapıntının təsviri

filament/tables paketində Attach və Associate actions zamanı relationship scope-un tam qorunmaması barədə advisory mövcuddur. Təsirlənən versiyalar istifadə olunduqda istifadəçi normalda görünməyən və ya tenant sərhədindən kənarda olan record-u əlaqələndirə bilər.

## Potensial təsir

Multi-tenant və rol əsaslı tətbiqlərdə horizontal authorization bypass, məlumat bütövlüyünün pozulması və başqa təşkilata aid record-ların əlaqələndirilməsi mümkün ola bilər. Risk həmin actions və custom scopes istifadəsindən asılıdır.

## Layihələr üzrə sübut

| Layihə | Təqdim edilmiş versiya | Manifest | FP |
|---|---|---|---|
| PDP Backend | guzzle 7.11.1; forms/tables 3.3.50; psr7 2.11.0 | pdp-backend/composer.lock və composer.json | 15% |
| MKA | guzzle 7.10.0; forms/tables 3.3.49; psr7 2.9.0 | etx/composer.lock və composer.json | 15% |
| CERT Backend / NCERT | guzzle 7.11.0; forms/tables 3.3.49; psr7 2.11.0 | cert-backend/composer.lock və composer.json | 35% |
| CERTKIDS | guzzle 7.10.0; forms/tables 3.3.47; psr7 2.8.0 | certkids/composer.lock və composer.json | 10% |

## Tövsiyə olunan düzəlişlər

- filament/tables patched versiyaya yüksəldilməlidir.
- Attach/Associate actions istifadə edən bütün resource-lar inventarlaşdırılmalı və authorization policy-ləri manual yoxlanılmalıdır.
- Server tərəfində tenant/owner scope hər mutation zamanı yenidən tətbiq edilməlidir.
- IDOR və cross-tenant association testləri security regression paketinə əlavə edilməlidir.

## Yenidən yoxlama meyarları

- Başqa tenant və ya scope xaricindəki record seçilə və əlaqələndirilə bilmir.
- composer audit GHSA-7q3w-xqjw-g3cr tapıntısını göstərmir.
- Authorization policy testləri həm UI, həm birbaşa request səviyyəsində uğurludur.
- Normal Attach/Associate funksionallığı pozulmur.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SCA-06 — PSR-7 method/version/reason phrase daxilində CR/LF qəbul edilməsi

| Yüksək | Dependency | CWE-1395 | OWASP A06:2021 | FP ehtimalı: layihəyə görə 10–40% |
|---|---|---|---|---|

| Paket | guzzlehttp/psr7 |
|---|---|
| Advisory | GHSA-vm85-hxw5-5432 / CVE-2026-55766 |
| Təsir olunan layihələr | PDP Backend, MKA, CERT Backend / NCERT, CERTKIDS |

## Tapıntının təsviri

guzzlehttp/psr7 paketinin təqdim edilmiş versiyalarında HTTP method, version və reason phrase daxilində CR/LF simvollarının qəbul edilməsi barədə header injection advisory-si mövcuddur. Dörd layihədə 2.8.0–2.11.0 aralığında müxtəlif versiyalar göstərilib.

## Potensial təsir

Untrusted input HTTP request/response komponentlərinə ötürülərsə, əlavə header daxil edilməsi, response splitting, cache poisoning və təhlükəsizlik nəzarətlərinin bypass edilməsi mümkün ola bilər. Real təsir data-flow və server/proxy davranışından asılıdır.

## Layihələr üzrə sübut

| Layihə | Təqdim edilmiş versiya | Manifest | FP |
|---|---|---|---|
| PDP Backend | guzzle 7.11.1; forms/tables 3.3.50; psr7 2.11.0 | pdp-backend/composer.lock və composer.json | 15% |
| MKA | guzzle 7.10.0; forms/tables 3.3.49; psr7 2.9.0 | etx/composer.lock və composer.json | 15% |
| CERT Backend / NCERT | guzzle 7.11.0; forms/tables 3.3.49; psr7 2.11.0 | cert-backend/composer.lock və composer.json | 35% |
| CERTKIDS | guzzle 7.10.0; forms/tables 3.3.47; psr7 2.8.0 | certkids/composer.lock və composer.json | 40% |

## Tövsiyə olunan düzəlişlər

- guzzlehttp/psr7 rəsmi advisory-də göstərilən patched versiyaya yüksəldilməlidir.
- HTTP method, version, reason phrase və header dəyərlərinə untrusted input ötürülən kod yolları audit edilməlidir.
- CR və LF simvolları tətbiq sərhədində rədd edilməlidir.
- Proxy, cache və web server konfiqurasiyasında response splitting müdafiələri yoxlanılmalıdır.

## Yenidən yoxlama meyarları

- composer audit GHSA-vm85-hxw5-5432 tapıntısını qaytarmır.
- CR/LF payload-ları exception və ya təhlükəsiz rejection ilə nəticələnir.
- Əlavə header yaradıla bilmir və response splitting baş vermir.
- HTTP client/server inteqrasiya testləri uğurludur.

MİLLİ KİBERTƏHLÜKƏSİZLİK AGENTLİYİ

KONFİDENSİAL

# SCA-07 — Local filesystem driver-də temporary signed URL expiration bypass

| Yüksək | Dependency | CWE-1395 | OWASP A06:2021 | FP ehtimalı: layihəyə görə 10–40% |
|---|---|---|---|---|

| Paket | laravel/framework |
|---|---|
| Advisory | GHSA-crmm-hgp2-wgrp / CVE təqdim edilməyib |
| Təsir olunan layihələr | PDP Backend, MKA, CERT Backend / NCERT, CERTKIDS |

## Tapıntının təsviri

laravel/framework paketində local filesystem driver istifadə edilən temporary signed URL-lərin expiration nəzarətinin bypass edilməsi barədə advisory təqdim olunub. Bütün layihələr composer.json daxilində ^12.0 constraint-i göstərir; resolved versiya composer.lock ilə təsdiqlənməlidir.

## Potensial təsir

Müvəqqəti link vaxtı bitdikdən sonra işlək qalarsa, məhdud müddət üçün paylaşılmış fayl və resurslara uzunmüddətli icazəsiz giriş mümkün ola bilər. Təsir local filesystem temporary URL funksiyasının istifadə olunmasından asılıdır.

## Layihələr üzrə sübut

| Layihə | Təqdim edilmiş versiya | Manifest | FP |
|---|---|---|---|
| PDP Backend | guzzle 7.11.1; forms/tables 3.3.50; psr7 2.11.0 | pdp-backend/composer.lock və composer.json | 20% |
| MKA | guzzle 7.10.0; forms/tables 3.3.49; psr7 2.9.0 | etx/composer.lock və composer.json | 20% |
| CERT Backend / NCERT | guzzle 7.11.0; forms/tables 3.3.49; psr7 2.11.0 | cert-backend/composer.lock və composer.json | 40% |
| CERTKIDS | guzzle 7.10.0; forms/tables 3.3.47; psr7 2.8.0 | certkids/composer.lock və composer.json | 20% |

## Tövsiyə olunan düzəlişlər

- laravel/framework patched release-ə yüksəldilməli və composer.lock yenilənməlidir.
- temporaryUrl və signed URL istifadə nöqtələri inventarlaşdırılmalı, filesystem driver-ları təsdiqlənməlidir.
- Həssas fayllar üçün əlavə server-side authorization və qısaömürlü token nəzarəti tətbiq edilməlidir.
- Köhnə signed URL-lərin cache və CDN qatlarında saxlanma siyasəti yoxlanılmalıdır.

## Yenidən yoxlama meyarları

- Expired URL expiration vaxtından sonra 403 və ya təhlükəsiz denial qaytarır.
- composer audit GHSA-crmm-hgp2-wgrp tapıntısını qaytarmır.
- Local və digər filesystem driver-lar üçün automated expiration testləri uğurludur.
- Fayl paylaşımı funksiyaları regression testdən keçir.

# Nəticə

Təqdim edilmiş nəticələrdə ən yüksək təcili risk CERTKIDS layihəsində repository-yə daxil edilmiş iki Google service-account private key-dir. Bu tapıntılar üçün əsas addım kod dəyişikliyi deyil, credential revocation, rotation, Git tarixçəsinin təmizlənməsi və audit log araşdırmasıdır.

Bütün dörd layihədə eyni yüksək riskli Composer advisory-lərinin təkrarlanması dependency management prosesinin mərkəzləşdirilməsinə ehtiyac olduğunu göstərir. Paketlərin yalnız bir dəfə lokal yenilənməsi kifayət deyil; patched minimum versiyalar, composer.lock nəzarəti, CI composer audit və periodik SCA monitorinqi təşkilati standart kimi tətbiq edilməlidir.

SAST üzrə upload və XSS tapıntıları manual validation tələb etsə də, tövsiyə olunan düzəlişlər təhlükəsiz dizayn prinsiplərinə uyğundur və false positive olsa belə müdafiə dərinliyini artırır. Bütün tapıntılar düzəlişdən sonra həm avtomatik skan, həm də məqsədli manual re-test ilə bağlanmalıdır.


MİLLİ
KİBERTƏHLÜKƏSİZLİK
AGENTLİYİ
Qaynar xətt:
1654
+994 12 598 90 90
www.cert.az
info@cert.az