V4 Giriş Nəzarəti

Nəzarət Məqsədi

Avtorizasiya, resurslara yalnız onlardan istifadə etməyə icazə verilmiş şəxslərə giriş imkanı vermək anlayışıdır. Təsdiqlənmiş tətbiqin aşağıdakı yüksək səviyyəli tələblərə cavab verdiyinə əmin olun:

• Resurslara daxil olan şəxslər bunu etmək üçün etibarlı etimadnaməyə malikdirlər.

• İstifadəçilər dəqiq müəyyən edilmiş rollar və imtiyazlar dəsti ilə əlaqələndirilir.

• Rol və icazə metadatası təkrar oxutmadan və ya müdaxilədən qorunur.

Təhlükəsizlik Yoxlama Tələbləri

V4.1 Ümumi Girişə Nəzarət Dizaynı

# Təsvir L1 L2 L3 CWE

**4.1.1** Tətbiqin etibarlı xidmət səviyyəsində girişə nəzarət qaydalarını tətbiq etdiyini yoxlayın, xüsusən müştəri tərəfi giriş nəzarəti mövcuddursa və onu keçə bilsəniz.

**4.1.2** Giriş nəzarəti tərəfindən istifadə edilən bütün istifadəçi və məlumat atributlarının və siyasət məlumatlarının xüsusi icazə verilmədiyi təqdirdə son istifadəçilər tərəfindən manipulyasiya edilə bilməyəcəyini yoxlayın.

**4.1.3** Ən az imtiyaz prinsipinin mövcud olduğunu yoxlayın - istifadəçilər yalnız xüsusi icazəyə malik olduqları funksiyalara, məlumat fayllarına, URL-lərə, nəzarətçilərə, xidmətlərə və digər resurslara daxil ola bilməlidirlər. Bu, saxtakarlıqdan və imtiyazların yüksəldilməsindən qorunmağı nəzərdə tutur. ( C7 )

**4.1.4** [SİLİNMİŞ, 4.1.3-NİN TƏKRİBİ]

**4.1.5** İstisna baş verdikdə daxil olmaqla, giriş nəzarətlərinin təhlükəsiz şəkildə uğursuz olduğunu yoxlayın. ( C10 )

V4.2 Əməliyyat Səviyyəsinə Giriş Nəzarəti

✓ ✓ ✓ 602 ✓ ✓ ✓ 639 ✓ ✓ ✓ 285

✓ ✓ ✓ 285

# Təsvir L1 L2 L3 CWE

**4.2.1** Həssas məlumatların və API-lərin başqasının qeydini yaratmaq və ya yeniləmək, hər kəsin qeydlərinə baxmaq və ya bütün qeydləri silmək kimi qeydlərin yaradılması, oxunması, yenilənməsi və silinməsini hədəfləyən Təhlükəsiz Birbaşa Obyekt Referansı (IDOR) hücumlarından qorunduğunu yoxlayın.

**4.2.2** Tətbiq və ya çərçivənin təsdiqlənmiş funksionallığı qorumaq üçün güclü anti-CSRF mexanizmi tətbiq etdiyini və effektiv anti-avtomatlaşdırma və ya anti-CSRF-in təsdiqlənməmiş funksionallığı qoruduğunu yoxlayın.

✓ ✓ ✓ 639 ✓ ✓ ✓ 352

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 36

V4.3 Digər Girişə Nəzarət Mülahizələri

# Təsvir L1 L2 L3 CWE

**4.3.1** İcazəsiz istifadənin qarşısını almaq üçün inzibati interfeyslərin müvafiq çoxfaktorlu autentifikasiyadan istifadə etdiyini yoxlayın.

**4.3.2** Qəsdən arzu olunmadıqda kataloqa baxışın söndürüldüyünü yoxlayın. Əlavə olaraq, proqramlar Thumbs.db, .DS\_Store, .git və ya .svn qovluqları kimi fayl və ya kataloq metadatasının aşkarlanmasına və ya açıqlanmasına icazə verməməlidir.

**4.3.3** Tətbiqin aşağı dəyərli sistemlər üçün əlavə icazəsi (yüksək və ya adaptiv autentifikasiya kimi) və/yaxud tətbiq riskinə və keçmiş saxtakarlığa uyğun olaraq anti-fırıldaqçılıq nəzarətini həyata keçirmək üçün yüksək dəyərli tətbiqlər üçün vəzifələrin ayrılmasına malik olduğunu yoxlayın.

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP Test Bələdçisi 4.0: Avtorizasiya

• OWASP Cheat Sheet: Girişə Nəzarət

• OWASP CSRF Cheat Sheet

• OWASP REST Cheat Sheet

✓ ✓ ✓ 419 ✓ ✓ ✓ 548

✓ ✓ 732

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 37



V5 Validasiya, Sanitizasiya və Kodlaşdırma

Nəzarət Məqsədi

Ən çox yayılmış veb tətbiqi təhlükəsizlik zəifliyi, müştəridən və ya ətraf mühitdən gələn girişi heç bir çıxış kodlaması olmadan birbaşa istifadə etməzdən əvvəl düzgün şəkildə təsdiqləməməkdir. Bu zəiflik saytlararası skript (XSS), SQL inyeksiyası, tərcüməçi inyeksiyası, locale/Unicode hücumları, fayl sistemi hücumları və bufer daşması kimi veb proqramlardakı demək olar ki, bütün əhəmiyyətli zəifliklərə gətirib çıxarır.

Təsdiqlənmiş tətbiqin aşağıdakı yüksək səviyyəli tələblərə cavab verdiyinə əmin olun:

• Girişin doğrulanması və çıxışın kodlaşdırılması arxitekturası inyeksiya hücumlarının qarşısını almaq üçün razılaşdırılmış boru kəmərinə malikdir. • Daxiletmə məlumatları güclü şəkildə yazılmış, təsdiqlənmiş, diapazon və ya uzunluq yoxlanılmış və ya ən pis halda təmizlənmiş və ya süzülmüşdür. • Çıxış məlumatları tərcüməçiyə mümkün qədər yaxın olan verilənlərin kontekstinə uyğun olaraq kodlaşdırılır və ya qaçırılır.

Müasir veb proqram arxitekturası ilə çıxış kodlaşdırması həmişəkindən daha vacibdir. Müəyyən ssenarilərdə möhkəm giriş təsdiqini təmin etmək çətindir, ona görə də parametrləşdirilmiş sorğular, avtomatik qaçan şablon çərçivələri və ya diqqətlə seçilmiş çıxış kodlaşdırması kimi daha təhlükəsiz API-dən istifadə tətbiqin təhlükəsizliyi üçün çox vacibdir.

V5.1 Giriş Təsdiqlənməsi

Müsbət icazə siyahıları və güclü məlumatların yazılmasından istifadə edərək düzgün şəkildə həyata keçirilən daxiletmənin yoxlanılması nəzarətləri bütün inyeksiya hücumlarının 90%-dən çoxunu aradan qaldıra bilər. Uzunluq və diapazon yoxlamaları bunu daha da azalda bilər. Tətbiq arxitekturası, dizayn sprintləri, kodlaşdırma, vahid və inteqrasiya testi zamanı təhlükəsiz daxiletmənin təsdiqlənməsinin qurulması tələb olunur. Bu elementlərin bir çoxunu nüfuzetmə testlərində tapmaq mümkün olmasa da, onların həyata keçirilməməsinin nəticələri adətən V5.3 - Çıxışın kodlaşdırılması və Enjeksiyonun qarşısının alınması tələblərində tapılır. Tərtibatçılara və təhlükəsiz kod rəyçilərinə bu bölməyə inyeksiyaların qarşısını almaq üçün bütün elementlər üçün L1 tələb olunan kimi yanaşmaq tövsiyə olunur.

# Təsvir L1 L2 L3 CWE

**5.1.1** Tətbiqin HTTP parametrlərinin çirklənməsi hücumlarına qarşı müdafiəyə malik olduğunu yoxlayın, xüsusən də proqram çərçivəsi sorğu parametrlərinin mənbəyi (GET, POST, kukilər, başlıqlar və ya mühit dəyişənləri) haqqında heç bir fərq qoymursa.

**5.1.2** Çərçivələrin kütləvi parametr təyinetmə hücumlarından qorunduğunu və ya tətbiqin təhlükəli parametr təyinatına qarşı qorunmaq üçün əks tədbirlərə malik olduğunu yoxlayın, məsələn, sahələrin özəl və ya oxşar işarələnməsi. ( C5 )

**5.1.3** Bütün daxiletmələrin (HTML forma sahələri, REST sorğuları, URL parametrləri, HTTP başlıqları, kukilər, toplu faylları, RSS lentləri və s.) müsbət yoxlamadan (siyahılara icazə verin) doğrulandığını yoxlayın. ( C5 )

**5.1.4** Strukturlaşdırılmış məlumatların icazə verilən simvollar, uzunluq və model (məsələn, kredit kartı nömrələri, e-poçt ünvanları, telefon nömrələri) daxil olmaqla müəyyən edilmiş sxemə uyğun olaraq güclü şəkildə yığıldığını və təsdiq edildiyini yoxlayın və ya iki əlaqəli sahənin ağlabatan olduğunu yoxlamaq, məsələn, şəhərətrafı və poçt/poçt indeksi uyğunluğu). ( C5 )

**5.1.5** URL yönləndirmələrinin və yönləndirmələrinin yalnız icazə siyahısında görünən təyinatlara icazə verdiyini və ya potensial etibarsız məzmuna yönləndirilərkən xəbərdarlıq göstərdiyini yoxlayın.

✓ ✓ ✓ 235

✓ ✓ ✓ 915 ✓ ✓ ✓ 20 ✓ ✓ ✓ 20

✓ ✓ ✓ 601

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 38



V5.2 Sanitizasiya və Sandboxing

# Təsvir L1 L2 L3 CWE

**5.2.1** WYSIWYG redaktorlarından və ya buna bənzər bütün etibarsız HTML daxiletmələrinin HTML təmizləyici kitabxanası və ya çərçivə funksiyası ilə düzgün şəkildə dezinfeksiya edildiyini yoxlayın. ( C5 )

**5.2.2** İcazə verilən simvollar və uzunluq kimi təhlükəsizlik tədbirlərini tətbiq etmək üçün strukturlaşdırılmamış məlumatların sanitarlaşdırıldığını yoxlayın.

**5.2.3** Tətbiqin SMTP və ya IMAP inyeksiyasından qorunmaq üçün poçt sistemlərinə keçməzdən əvvəl istifadəçi daxiletməsini sanitarlaşdırdığını yoxlayın.

**5.2.4** Tətbiqin eval() və ya digər dinamik kod icra funksiyalarından istifadə etmədiyini yoxlayın. Alternativ olmadıqda, daxil edilən hər hansı istifadəçi daxiletməsi icra edilməzdən əvvəl təmizlənməlidir və ya qum qutusuna salınmalıdır.

**5.2.5** Daxil edilən hər hansı istifadəçi daxiletməsinin sanitarlaşdırılmış və ya qum qutusuna salınmasını təmin etməklə tətbiqin şablon inyeksiya hücumlarından qorunduğunu yoxlayın.

**5.2.6** Fayl adları və URL daxiletmə sahələri kimi etibarsız verilənləri və ya HTTP fayl metadatasını təsdiq edərək və ya təmizləyərək tətbiqin SSRF hücumlarından qoruduğunu yoxlayın və protokolların, domenlərin, yolların və portların icazə siyahılarından istifadə edin.

**Ölçüləndirilə bilən Vektor Qrafikası** (SVG) skript məzmununu, xüsusən də daxili skriptlərdən və xarici Obyektdən yaranan XSS ilə əlaqədar olaraq, dezinfeksiya etdiyini, qeyri-aktiv etdiyini və ya qum qutusunda saxladığını yoxlayın.

**5.2.8** Tətbiqin Markdown, CSS və ya XSL üslub cədvəlləri, BBCode və ya oxşarı kimi istifadəçi tərəfindən təmin edilmiş skript və ya ifadə şablonu dili məzmununu dezinfeksiya etdiyini, söndürdüyünü və ya qum qutusunda saxladığını yoxlayın.

V5.3 Çıxışın kodlaşdırılması və inyeksiyanın qarşısının alınması

✓ ✓ ✓ 116 ✓ ✓ ✓ 138 ✓ ✓ ✓ 147 ✓ ✓ ✓ 95

✓ ✓ ✓ 94 ✓ ✓ ✓ 918

✓ ✓ ✓ 159 ✓ ✓ ✓ 94

İstifadə olunan tərcüməçiyə yaxın və ya bitişik çıxış kodlaşdırması hər hansı tətbiqin təhlükəsizliyi üçün çox vacibdir. Tipik olaraq, çıxış kodlaşdırması davamlı deyil, lakin dərhal istifadə üçün müvafiq çıxış kontekstində çıxışı təhlükəsiz etmək üçün istifadə olunur. Şifrəni çıxara bilməmək təhlükəsiz, inyeksiya edilə bilən və təhlükəli tətbiq ilə nəticələnəcək.

# Təsvir L1 L2 L3 CWE

**5.3.1** Çıxış kodlaşdırmasının tərcüməçi və tələb olunan kontekst üçün uyğun olduğunu yoxlayın. Məsələn, kontekst tələb etdiyi kimi HTML dəyərləri, HTML atributları, JavaScript, URL parametrləri, HTTP başlıqları, SMTP və digərləri üçün kodlayıcılardan istifadə edin, xüsusən etibarsız girişlərdən (məsələn, Unicode və ya apostroflu adlar, məsələn,ねこvə ya O'Hara) . ( C4 )

**5.3.2** Hər hansı Unicode simvol nöqtəsinin etibarlı və təhlükəsiz şəkildə idarə olunması üçün çıxış kodlaşdırmasının istifadəçinin seçdiyi simvol dəstini və dilini qoruduğunu yoxlayın. ( C4 )

**5.3.3** Kontekstdən xəbərdar olan, tercihen avtomatlaşdırılmış və ya ən pis halda əl ilə çıxışın əks olunan, saxlanılan və DOM əsaslı XSS-dən qorunduğunu yoxlayın. ( C4 )

**5.3.4** Məlumat seçimi və ya verilənlər bazası sorğularının (məsələn, SQL, HQL, ORM, NoSQL) parametrləşdirilmiş sorğulardan, ORM-lərdən, obyekt çərçivələrindən istifadə etdiyini və ya verilənlər bazasına inyeksiya hücumlarından başqa şəkildə qorunduğunu yoxlayın. ( C3 )

✓ ✓ ✓ 116

✓ ✓ ✓ 176 ✓ ✓ ✓ 79 ✓ ✓ ✓ 89

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 39



# Təsvir L1 L2 L3 CWE

**5.3.5** Parametrləşdirilmiş və ya daha təhlükəsiz mexanizmlərin mövcud olmadığı yerlərdə, SQL inyeksiyasından qorunmaq üçün qaçan SQL-in istifadəsi kimi inyeksiya hücumlarından qorunmaq üçün kontekst üzrə xüsusi çıxış kodlaşdırmasının istifadə edildiyini yoxlayın. ( C3, C4 )

**5.3.6** Tətbiqin JSON inyeksiya hücumlarından, JSON qiymətləndirmə hücumlarından və JavaScript ifadə qiymətləndirməsindən qorunduğunu yoxlayın. ( C4 )

**5.3.7 Tətbiqin** LDAP inyeksiya zəifliklərindən qorunduğunu və ya LDAP inyeksiyasının qarşısını almaq üçün xüsusi təhlükəsizlik nəzarətlərinin həyata keçirildiyini yoxlayın. ( C4 )

**5.3.8** Tətbiqin ƏS əmrlərinin inyeksiyasından qorunduğunu və əməliyyat sistemi çağırışlarının parametrləşdirilmiş ƏS sorğularından istifadə etdiyini və ya kontekstli komanda xətti çıxış kodlaşdırmasından istifadə etdiyini yoxlayın. ( C4 )

**5.3.9 Tətbiqin** Local File Inclusion (LFI) və ya Remote File Inclusion (RFI) hücumlarından qorunduğunu yoxlayın.

**5.3.10** Tətbiqin XPath injection və ya XML injection hücumlarından qoruduğunu yoxlayın. ( C4 )

✓ ✓ ✓ 89

✓ ✓ ✓ 830 ✓ ✓ ✓ 90

✓ ✓ ✓ 78

✓ ✓ ✓ 829 ✓ ✓ ✓ 643

Qeyd: Parametrləşdirilmiş sorğulardan istifadə etmək və ya SQL-dən qaçmaq həmişə kifayət etmir; cədvəl və sütun adları, ORDER BY və s., qaçırmaq olmaz. Qaçan istifadəçi tərəfindən təmin edilmiş məlumatların bu sahələrə daxil edilməsi uğursuz sorğular və ya SQL inyeksiyası ilə nəticələnir.

Qeyd: SVG formatı demək olar ki, bütün kontekstlərdə ECMA skriptinə açıq şəkildə icazə verir, ona görə də bütün SVG XSS vektorlarını tamamilə bloklamaq mümkün olmaya bilər. SVG yükləməsi tələb olunarsa, uğurlu XSS-in tətbiqi ələ keçirməsinin qarşısını almaq üçün ya bu yüklənmiş faylları mətn/düz kimi təqdim etməyi və ya istifadəçi tərəfindən təmin edilmiş ayrıca məzmun domenindən istifadə etməyi tövsiyə edirik.

V5.4 Yaddaş, String və İdarə olunmayan Kod

Aşağıdakı tələblər yalnız proqram sistem dilindən və ya idarə olunmayan koddan istifadə etdikdə tətbiq olunacaq. # Təsvir L1 L2 L3 CWE

**5.4.1** Tətbiqin yığın, bufer və ya yığın daşqınlarını aşkar etmək və ya qarşısını almaq üçün yaddaş üçün təhlükəsiz sətir, daha təhlükəsiz yaddaş surəti və göstərici arifmetikasından istifadə etdiyini yoxlayın.

**5.4.2** Format sətirlərinin potensial düşmən girişini qəbul etmədiyini və sabit olduğunu yoxlayın.

**5.4.3** Tam ədədlərin çoxalmasının qarşısını almaq üçün işarə, diapazon və daxiletmənin doğrulama üsullarından istifadə olunduğunu yoxlayın.

✓ ✓ 120 ✓ ✓ 134 ✓ ✓ 190

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 40



V5.5 Serializasiyanın qarşısının alınması

# Təsvir L1 L2 L3 CWE

**5.5.1** Düşmən obyektin yaradılmasının və ya məlumatların dəyişdirilməsinin qarşısını almaq üçün seriallaşdırılmış obyektlərin bütövlüyü yoxlamalarından istifadə etdiyini və ya şifrələndiyini yoxlayın. ( C5 )

**5.5.2** Tətbiqin XML təhlilçilərini yalnız mümkün olan ən məhdudlaşdırıcı konfiqurasiyadan istifadə etmək üçün düzgün məhdudlaşdırdığını yoxlayın və XML eXternal Entity (XXE) hücumlarının qarşısını almaq üçün xarici obyektlərin həlli kimi təhlükəli funksiyaların söndürülməsini təmin edin.

**5.5.3** Etibarsız məlumatların sıradan çıxarılmasının qarşısının alındığını və ya həm fərdi kodlarda, həm də üçüncü tərəf kitabxanalarında (məsələn, JSON, XML və YAML təhlilçiləri kimi) qorunduğunu yoxlayın.

**5.5.4** Doğrulayın ki, JSON brauzerlərdə və ya JavaScript əsaslı backendlərdə təhlil edilərkən, JSON sənədini təhlil etmək üçün JSON.parse istifadə olunur. JSON-u təhlil etmək üçün eval() istifadə etməyin.

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP Test Bələdçisi 4.0: Daxiletmə Qiymətləndirmə Testi

• OWASP Fırıldaq Vərəqi: Daxiletmə Qiymətləndirməsi

• OWASP Test Bələdçisi 4.0: HTTP Parametrinin Çirklənməsi üçün Test • OWASP LDAP Injection Cheat Sheet

• OWASP Test Bələdçisi 4.0: Müştəri Tərəfindən Test

• OWASP Saytlararası Skriptin qarşısının alınması Fırıldaq vərəqi

• OWASP DOM Əsaslı Saytlararası Skriptlərin qarşısının alınması Fırıldaq vərəqi • OWASP Java Kodlaşdırma Layihəsi

• OWASP Kütləvi Təyinatın qarşısının alınması Fırıldaq vərəqi

• DOMPurify - Müştəri tərəfində HTML Təmizləmə Kitabxanası

• XML Xarici Müəssisənin (XXE) Qarşısının Alınması Fırıldaq Vərəqi

Avtomatik qaçış haqqında ətraflı məlumat üçün baxın:

• Şablon sistemlərində kontekstdən xəbərdar olan avtomatik qaçış yolu ilə XSS-nin azaldılması • AngularJS Strict Contextual Ecaping

• AngularJS ngBind

• Bucaqlı sanitarizasiya

• Bucaq təhlükəsizlik

• ReactJS Ecaping

• Dinamik olaraq təyin olunan obyekt atributlarının düzgün idarə olunmayan modifikasiyası Deserializasiya haqqında daha çox məlumat üçün baxın:

• OWASP Deserialization Cheat Sheet

• Etibarsız Məlumat Bələdçisinin OWASP Seriyadan çıxarılması

✓ ✓ ✓ 502 ✓ ✓ ✓ 611

✓ ✓ ✓ 502 ✓ ✓ ✓ 95

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 41



V6 Saxlanan Kriptoqrafiya

Nəzarət Məqsədi

Təsdiqlənmiş tətbiqin aşağıdakı yüksək səviyyəli tələblərə cavab verdiyinə əmin olun:

• Bütün kriptoqrafik modullar təhlükəsiz şəkildə uğursuz olur və səhvlər düzgün idarə olunur. • Uyğun təsadüfi ədədlər generatorundan istifadə edilir.

• Açarlara giriş təhlükəsiz şəkildə idarə olunur.

V6.1 Məlumatların Təsnifatı

Ən vacib aktiv proqram tərəfindən işlənmiş, saxlanılan və ya ötürülən məlumatlardır. Hər hansı saxlanılan məlumatın məlumatların qorunması ehtiyaclarını düzgün təsnif etmək üçün həmişə məxfiliyə təsirin qiymətləndirilməsini həyata keçirin.

# Təsvir L1 L2 L3 CWE

**6.1.1** Şəxsi Müəyyənləşdirilə bilən Məlumat (PII), həssas şəxsi məlumatlar və ya Aİ-nin GDPR-ə tabe olacağı ehtimal edilən məlumatlar kimi tənzimlənən şəxsi məlumatların istirahət zamanı şifrələnmiş şəkildə saxlandığını yoxlayın.

**6.1.2** Tənzimlənən sağlamlıq məlumatlarının tibbi qeydlər, tibbi cihaz təfərrüatları və ya anonimləşdirilmiş tədqiqat qeydləri kimi istirahət zamanı şifrələnmiş şəkildə saxlandığını yoxlayın.

**6.1.3** Maliyyə hesabları, defolt və ya kredit tarixçəsi, vergi qeydləri, ödəniş tarixçəsi, benefisiarlar və ya anonimləşdirilmiş bazar və ya araşdırma qeydləri kimi tənzimlənən maliyyə məlumatlarının istirahət zamanı şifrələnmiş şəkildə saxlandığını yoxlayın.

V6.2 Alqoritmlər

✓ ✓ 311

✓ ✓ 311 ✓ ✓ 311

Kriptoqrafiya sahəsində son nailiyyətlər o deməkdir ki, əvvəllər təhlükəsiz olan alqoritmlər və açar uzunluqları artıq təhlükəsiz və ya məlumatların qorunması üçün kifayət deyil. Ona görə də alqoritmləri dəyişmək mümkün olmalıdır.

Baxmayaraq ki, bu bölmə asanlıqla nüfuzetmə testindən keçmir, tərtibatçılar L1 elementlərinin əksəriyyətində əskik olmasına baxmayaraq, bütün bu bölməni məcburi hesab etməlidirlər.

# Təsvir L1 L2 L3 CWE

**6.2.1** Bütün kriptoqrafik modulların təhlükəsiz şəkildə uğursuz olduğunu və xətaların Padding Oracle hücumlarına imkan verməyən şəkildə idarə olunduğunu yoxlayın.

**6.2.2** Xüsusi kodlaşdırılmış kriptoqrafiya əvəzinə sənayedə təsdiqlənmiş və ya hökumət tərəfindən təsdiqlənmiş kriptoqrafik alqoritmlər, rejimlər və kitabxanalardan istifadə edildiyini yoxlayın. ( C8 )

**6.2.3** Ən son məsləhətlərdən istifadə etməklə şifrələmənin başlanğıc vektorunun, şifrə konfiqurasiyası və blok rejimlərinin təhlükəsiz şəkildə konfiqurasiya edildiyini yoxlayın.

**6.2.4** Təsadüfi nömrələrin, şifrələmə və ya heşinq alqoritmlərinin, açar uzunluqlarının, dövrələrin, şifrələrin və ya rejimlərin kriptoqrafik fasilələrdən qorunmaq üçün istənilən vaxt yenidən konfiqurasiya edilə, təkmilləşdirilə və ya dəyişdirilə biləcəyini yoxlayın. ( C8 )

**6.2.5** Məlum təhlükəsiz blok rejimlərinin (yəni ECB və s.), doldurma rejimlərinin (yəni PKCS#1 v1.5 və s.), kiçik blok ölçüləri olan şifrələrin (yəni Triple-DES, Blowfish və s.) və zəif hashing alqoritmləri (yəni MD5, SHA1 və s.) geriyə uyğunluq tələb olunmadığı təqdirdə istifadə edilmir.

✓ ✓ ✓ 310 ✓ ✓ 327

✓ ✓ 326

✓ ✓ 326

✓ ✓ 326

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 42



# Təsvir L1 L2 L3 CWE

**6.2.6** Təsdiq edin ki, qeyri-şəxslər, başlatma vektorları və digər birdəfəlik istifadə nömrələri verilmiş şifrələmə açarı ilə bir dəfədən çox istifadə edilməməlidir. Yaratma üsulu istifadə olunan alqoritmə uyğun olmalıdır.

**6.2.7** Şifrələnmiş məlumatın imzalar, təsdiqlənmiş şifrə rejimləri və ya HMAC vasitəsilə autentifikasiya olunduğunu yoxlayın ki, şifrəli mətnin icazəsiz şəxs tərəfindən dəyişdirilməməsinə əmin olun.

**6.2.8 Məlumat sızmasının** qarşısını almaq üçün bütün kriptoqrafik əməliyyatların müqayisələrdə, hesablamalarda və ya qaytarmalarda “qısaqapanma” əməliyyatları olmadan sabit vaxtda olduğunu yoxlayın.

V6.3 Təsadüfi Dəyərlər

✓ ✓ 326 ✓ 326

✓ 385

Həqiqi Pseudo-təsadüfi Nömrələrin Yaradılması (PRNG) düzəltmək olduqca çətindir. Ümumiyyətlə, sistem daxilində yaxşı entropiya mənbələri həddindən artıq istifadə edildikdə tez tükənəcək, lakin daha az təsadüfi olan mənbələr proqnozlaşdırıla bilən açarlara və sirlərə səbəb ola bilər.

# Təsvir L1 L2 L3 CWE

**6.3.1** Bütün təsadüfi ədədlərin, təsadüfi fayl adlarının, təsadüfi GUID-lərin və təsadüfi sətirlərin kriptoqrafik modulun təsdiq edilmiş kriptoqrafik cəhətdən təhlükəsiz təsadüfi ədəd generatorundan istifadə edərək yaradıldığını yoxlayın, o zaman bu təsadüfi dəyərlər təcavüzkar tərəfindən təxmin edilə bilməz.

**6.3.2** Təsadüfi GUID-lərin GUID v4 alqoritmi və Kriptoqrafik cəhətdən təhlükəsiz Pseudo-təsadüfi Nömrələr Generatoru (CSPRNG) istifadə edərək yaradıldığını yoxlayın. Digər psevdo-təsadüfi ədəd generatorlarından istifadə etməklə yaradılmış GUID-lər proqnozlaşdırıla bilər.

**6.3.3** Tətbiq ağır yük altında olduqda belə təsadüfi ədədlərin düzgün entropiya ilə yaradıldığını və ya belə şəraitdə tətbiqin zərif şəkildə pisləşdiyini yoxlayın.

V6.4 Gizli İdarəetmə

✓ ✓ 338 ✓ ✓ 338 ✓ 338

Baxmayaraq ki, bu bölmə asanlıqla nüfuzetmə testindən keçmir, tərtibatçılar L1 elementlərinin əksəriyyətində əskik olmasına baxmayaraq, bütün bu bölməni məcburi hesab etməlidirlər.

# Təsvir L1 L2 L3 CWE

**6.4.1** Sirləri təhlükəsiz şəkildə yaratmaq, saxlamaq, onlara girişi idarə etmək və məhv etmək üçün açar anbarı kimi sirlərin idarə edilməsi həllinin istifadə edildiyini yoxlayın. ( C8 )

**6.4.2** Əsas materialın tətbiqə məruz qalmadığını, əksinə kriptoqrafik əməliyyatlar üçün anbar kimi təcrid olunmuş təhlükəsizlik modulundan istifadə etdiyini yoxlayın. ( C8 )

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP Test Bələdçisi 4.0: Zəif Kriptoqrafiya üçün sınaq

• OWASP Cheat Sheet: Kriptoqrafik Saxlama

• FIPS 140-2

✓ ✓ 798 ✓ ✓ 320

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 43



V7 Xətaların İdarə Edilməsi və Qeydiyyatı

Nəzarət Məqsədi

Səhvlərin idarə edilməsi və qeydiyyatının əsas məqsədi istifadəçi, idarəçilər və insidentlərə cavab verən qruplar üçün faydalı məlumat verməkdir. Məqsəd böyük miqdarda loglar deyil, atılan səs-küydən daha çox siqnala malik yüksək keyfiyyətli loglar yaratmaqdır.

Yüksək keyfiyyətli qeydlər çox vaxt həssas məlumatları ehtiva edir və yerli məlumatların məxfiliyi qanunlarına və ya direktivlərinə uyğun olaraq qorunmalıdır. Bura daxil edilməlidir:

• Xüsusi tələb olunmadıqda, həssas məlumatların toplanmaması və ya daxil edilməməsi.

• Daxil edilmiş bütün məlumatların etibarlı şəkildə idarə olunmasını və məlumat təsnifatına uyğun olaraq mühafizəsini təmin etmək. • Günlüklərin əbədi olaraq saxlanmamasını, lakin mümkün qədər qısa olan mütləq ömür müddətinin olmasını təmin etmək.

Jurnallar tərifi ölkədən ölkəyə dəyişən şəxsi və ya həssas məlumatları ehtiva edirsə, qeydlər tətbiqin saxladığı ən həssas məlumatlardan birinə çevrilir və beləliklə, özlüyündə təcavüzkarlar üçün çox cəlbedici olur.

Tətbiqin təhlükəsiz şəkildə uğursuz olmasını və səhvlərin lazımsız məlumatları açıqlamamasını təmin etmək də vacibdir.

V7.1 Giriş Məzmunu

Həssas məlumatları qeyd etmək təhlükəlidir - qeydlər özləri məxfiləşir, bu o deməkdir ki, onlar şifrələnməlidir, saxlama siyasətlərinə tabe olmalıdır və təhlükəsizlik auditlərində açıqlanmalıdır. Jurnallarda yalnız zəruri məlumatların saxlandığından və əlbəttə ki, heç bir ödənişin, etimadnamələrin (sessiya nişanları daxil olmaqla), həssas və ya şəxsiyyəti müəyyən edən məlumatların olmamasından əmin olun.

V7.1 OWASP Top 10 2017:A10-u əhatə edir. 2017:A10 və bu bölmə penetrasiya üçün sınaqdan keçirilmədiyi üçün bu, aşağıdakılar üçün vacibdir:

• Tərtibatçılar bu bölməyə tam uyğunluğu təmin etməlidirlər, sanki bütün elementlər L1 kimi qeyd edilmişdir. • Müsahibə, skrinşotlar və ya təsdiqləmə vasitəsilə V7.1-dəki bütün elementlərin tam uyğunluğunu yoxlamaq üçün nüfuzetmə testçiləri # Təsvir L1 L2 L3 CWE

**7.1.1** Tətbiqin etimadnamələri və ya ödəniş təfərrüatlarını daxil etmədiyini yoxlayın. Sessiya nişanları yalnız geri dönməz, heşlənmiş formada jurnallarda saxlanmalıdır. ( C9, C10 )

**7.1.2** Tətbiqin yerli məxfilik qanunları və ya müvafiq təhlükəsizlik siyasəti ilə müəyyən edilmiş digər həssas məlumatları qeyd etmədiyini yoxlayın. ( C9 )

**7.1.3** Tətbiqin uğurlu və uğursuz autentifikasiya hadisələri, girişə nəzarət uğursuzluqları, sıradan çıxarma uğursuzluqları və daxilolma doğrulama uğursuzluqları daxil olmaqla, təhlükəsizliyə aid hadisələri qeyd etdiyini yoxlayın. ( C5, C7 )

**7.1.4** Hər bir jurnal hadisəsinin hadisənin baş verdiyi zaman qrafikinin təfərrüatlı tədqiqinə imkan verəcək zəruri məlumatları ehtiva etdiyini yoxlayın. ( C9 )

✓ ✓ ✓ 532

✓ ✓ ✓ 532 ✓ ✓ 778

✓ ✓ 778

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 44



V7.2 Giriş Emalı

Audit hadisələri, triaj və eskalasiya üçün vaxtında qeydiyyat çox vacibdir. Tətbiqin qeydlərinin aydın olduğundan və yerli olaraq asanlıqla izlənilə və təhlil oluna biləcəyinə və ya jurnalın uzaqdan monitorinq sisteminə göndərilməsinə əmin olun.

V7.2 OWASP Top 10 2017:A10-u əhatə edir. 2017:A10 və bu bölmə penetrasiya üçün sınaqdan keçirilmədiyi üçün bu, aşağıdakılar üçün vacibdir:

• Tərtibatçılar bu bölməyə tam uyğunluğu təmin etməlidirlər, sanki bütün elementlər L1 kimi qeyd edilmişdir. • Müsahibə, skrinşotlar və ya təsdiqləmə vasitəsilə V7.2-dəki bütün elementlərin tam uyğunluğunu yoxlamaq üçün nüfuzetmə testçiləri # Təsvir L1 L2 L3 CWE

**7.2.1** Həssas seans nişanları və ya parolları saxlamadan bütün autentifikasiya qərarlarının qeydiyyata alındığını yoxlayın. Buraya təhlükəsizlik araşdırmaları üçün lazım olan müvafiq metadata ilə sorğular daxil edilməlidir.

**7.2.2** Bütün girişə nəzarət qərarlarının qeyd oluna biləcəyini və bütün uğursuz qərarların qeydiyyata alındığını yoxlayın. Buraya təhlükəsizlik araşdırmaları üçün lazım olan müvafiq metadata ilə sorğular daxil edilməlidir.

V7.3 Giriş Mühafizəsi

✓ ✓ 778 ✓ ✓ 285

Təhqiqat və təqiblər üçün əhəmiyyətsiz şəkildə dəyişdirilə və ya silinə bilən qeydlər yararsızdır. Qeydlərin açıqlanması proqram və ya onun ehtiva etdiyi məlumatlar haqqında daxili təfərrüatları ifşa edə bilər. Qeydləri icazəsiz açıqlamadan, dəyişdirilmədən və ya silinmədən qoruyarkən diqqətli olmaq lazımdır.

# Təsvir L1 L2 L3 CWE

**7.3.1** Jurnalın inyeksiyasının qarşısını almaq üçün bütün qeyd komponentlərinin məlumatları müvafiq şəkildə kodlaşdırdığını yoxlayın. ( C9 )

**7.3.2** [SİLİNMİŞ, 7.3.1-NİN TƏKRİBİ]

**7.3.3** Təhlükəsizlik jurnallarının icazəsiz giriş və dəyişikliklərdən qorunduğunu yoxlayın. ( C9 )

**7.3.4** Vaxt mənbələrinin düzgün vaxt və saat qurşağı ilə sinxronlaşdırıldığını yoxlayın. Sistemlər hadisədən sonrakı məhkəmə-tibbi analizə kömək etmək üçün qlobaldırsa, yalnız UTC-də daxil olmağı ciddi şəkildə nəzərdən keçirin. ( C9 )

✓ ✓ 117

✓ ✓ 200 ✓ ✓

Qeyd: Login kodlaşdırılmasını (7.3.1) avtomatlaşdırılmış dinamik alətlər və nüfuz testlərindən istifadə etməklə sınaqdan keçirmək və nəzərdən keçirmək çətindir, lakin memarlar, tərtibatçılar və mənbə kodunu nəzərdən keçirənlər bunu L1 tələbi hesab etməlidirlər.

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 45



V7.4 Xətaların idarə edilməsi

Səhvlərin idarə edilməsinin məqsədi proqrama monitorinq, triaj və eskalasiya üçün təhlükəsizliklə bağlı müvafiq hadisələri təmin etməyə imkan verməkdir. Məqsəd qeydlər yaratmaq deyil. Təhlükəsizliyə bağlı hadisələri qeyd edərkən, qeydin məqsədinin olduğundan və onun SIEM və ya analiz proqramı ilə fərqlənə biləcəyindən əmin olun.

# Təsvir L1 L2 L3 CWE

**7.4.1** Ümumi mesajın gözlənilməz və ya təhlükəsizlik baxımından həssas xəta baş verdikdə göstərildiyini yoxlayın, ola bilsin ki, dəstək personalının araşdırmaq üçün istifadə edə biləcəyi unikal ID ilə. ( C10 )

**7.4.2** Gözlənilən və gözlənilməz xəta şərtlərini nəzərə almaq üçün kod bazasında istisnaların idarə edilməsinin (və ya funksional ekvivalentinin) istifadə edildiyini yoxlayın. ( C10 )

**7.4.3 Bütün idarə olunmayan istisnaları tutacaq** "son çarə" səhv idarəedicisinin müəyyən edildiyini yoxlayın. ( C10 )

✓ ✓ ✓ 210

✓ ✓ 544

✓ ✓ 431

Qeyd: Swift və Go kimi müəyyən dillər - və ümumi dizayn təcrübəsi vasitəsilə - bir çox funksional dillər istisnaları və ya son çarə hadisə idarəçilərini dəstəkləmir. Bu halda, memarlar və tərtibatçılar tətbiqlərin müstəsna, gözlənilməz və ya təhlükəsizliklə bağlı hadisələri təhlükəsiz şəkildə idarə edə bilməsini təmin etmək üçün nümunə, dil və ya çərçivəyə uyğun üsuldan istifadə etməlidirlər.

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP Test Bələdçisi 4.0 məzmunu: Səhvlərin idarə edilməsi üçün sınaq

• Səhv mesajları haqqında OWASP Authentication Cheat Sheet bölməsi

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 46



V8 Məlumat Mühafizəsi

Nəzarət Məqsədi

Sağlam məlumatların qorunması üçün üç əsas element var: Məxfilik, Dürüstlük və Əlçatanlıq (CIA). Bu standart güman edir ki, verilənlərin mühafizəsi gücləndirilmiş və kifayət qədər qorunmaya malik olan server kimi etibarlı sistemdə tətbiq edilir.

Tətbiqlər bütün istifadəçi cihazlarının hansısa şəkildə təhlükəyə məruz qaldığını güman etməlidir. Tətbiq paylaşılan kompüterlər, telefonlar və planşetlər kimi təhlükəli cihazlarda həssas məlumatları ötürən və ya saxladığı halda, proqram bu cihazlarda saxlanılan məlumatların şifrələnməsinə və asanlıqla qeyri-qanuni əldə edilə, dəyişdirilə və ya açıqlana bilməyəcəyinə əmin olmaq üçün məsuliyyət daşıyır.

Təsdiqlənmiş tətbiqin aşağıdakı yüksək səviyyəli məlumatların qorunması tələblərinə cavab verdiyinə əmin olun:

• Məxfilik: Məlumat həm tranzit zamanı, həm də saxlanarkən icazəsiz müşahidədən və ya açıqlamadan qorunmalıdır.

• Dürüstlük: Məlumatlar icazəsiz hücumçular tərəfindən zərərli şəkildə yaradılmaqdan, dəyişdirilməkdən və ya silinməkdən qorunmalıdır.

• Əlçatanlıq: Məlumat tələb olunduqda səlahiyyətli istifadəçilər üçün əlçatan olmalıdır.

V8.1 Ümumi Məlumat Mühafizəsi

# Təsvir L1 L2 L3 CWE

**8.1.1** Tətbiqin həssas məlumatların yük balanslaşdırıcıları və proqram keşləri kimi server komponentlərində saxlanmasından qoruduğunu yoxlayın.

**8.1.2** Serverdə saxlanılan həssas məlumatların bütün keşlənmiş və ya müvəqqəti nüsxələrinin icazəsiz girişdən qorunduğunu və ya səlahiyyətli istifadəçi həssas məlumatlara daxil olduqdan sonra təmizləndiyini/etibarsız olduğunu yoxlayın.

**8.1.3** Tətbiqin sorğudakı gizli sahələr, Ajax dəyişənləri, kukilər və başlıq dəyərləri kimi parametrlərin sayını minimuma endirdiyini yoxlayın.

**8.1.4** Tətbiqin IP, istifadəçi, saat və ya gündə cəmi və ya tətbiq üçün mənası olan hər hansı bir sorğu kimi anormal sayda sorğuları aşkarlaya və xəbərdar edə biləcəyini yoxlayın.

**8.1.5** Mühüm məlumatların müntəzəm ehtiyat nüsxələrinin çıxarılmasını və məlumatların sınaq bərpasının həyata keçirildiyini yoxlayın.

**8.1.6** Məlumatların oğurlanmasının və ya korlanmasının qarşısını almaq üçün ehtiyat nüsxələrin təhlükəsiz şəkildə saxlandığını yoxlayın.

V8.2 Müştəri tərəfində məlumatların qorunması

✓ ✓ 524 ✓ ✓ 524

✓ ✓ 233 ✓ ✓ 770

✓ 19

✓ 19

# Təsvir L1 L2 L3 CWE

**8.2.1** Həssas məlumatların müasir brauzerlərdə yaddaşda saxlanmaması üçün tətbiqin kifayət qədər anti-keş başlıqlar qurduğunu yoxlayın.

**8.2.2** Brauzer yaddaşında saxlanılan verilənlərin (localStorage, sessionStorage, IndexedDB və ya kukilər kimi) həssas məlumatları ehtiva etmədiyini yoxlayın.

**8.2.3** Müştəri və ya sessiya dayandırıldıqdan sonra təsdiqlənmiş məlumatların DOM brauzeri kimi müştəri yaddaşından silindiyini yoxlayın.

✓ ✓ ✓ 525 ✓ ✓ ✓ 922 ✓ ✓ ✓ 922

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 47



V8.3 Həssas Şəxsi Məlumat

Bu bölmə həssas məlumatların icazəsiz, xüsusən də toplu miqdarda yaradılması, oxunması, yenilənməsi və ya silinməsindən qorunmasına kömək edir.

Bu bölməyə uyğunluq V4 Giriş Nəzarəti və xüsusilə V4.2 ilə uyğunluğu nəzərdə tutur. Məsələn, icazəsiz yeniləmələrdən və ya həssas şəxsi məlumatların açıqlanmasından qorunmaq üçün V4.2.1-ə riayət etmək lazımdır. Tam əhatə üçün bu bölməyə və V4-ə əməl edin.

Qeyd: Avstraliya Məxfilik Prinsipləri APP-11 və ya GDPR kimi məxfilik qaydaları və qanunları tətbiqlərin həssas şəxsi məlumatların saxlanması, istifadəsi və ötürülməsinin həyata keçirilməsinə yanaşma tərzinə birbaşa təsir göstərir. Bu, ağır cəzalardan tutmuş sadə məsləhətlərə qədər dəyişir. Zəhmət olmasa yerli qanun və qaydalarınızla məsləhətləşin və tələb olunduqda məxfilik üzrə ixtisaslı mütəxəssis və ya hüquqşünasla məsləhətləşin.

# Təsvir L1 L2 L3 CWE

**8.3.1** Həssas verilənlərin HTTP mesajının mətnində və ya başlıqlarında serverə göndərildiyini və hər hansı HTTP felindən olan sorğu sətirinin parametrlərində həssas məlumatların olmadığını yoxlayın.

✓ ✓ ✓ 319

**8.3.2** İstifadəçilərin tələb əsasında məlumatlarını silmək və ya ixrac etmək üsulunun olduğunu yoxlayın. ✓ ✓ ✓ 212

**8.3.3** İstifadəçilərə təqdim edilmiş şəxsi məlumatların toplanması və istifadəsi ilə bağlı aydın dillə təmin olunduğunu və istifadəçilərin hər hansı şəkildə istifadə edilməzdən əvvəl həmin məlumatların istifadəsi üçün razılıq verdiyini yoxlayın.

**8.3.4** Tətbiq tərəfindən yaradılmış və emal edilmiş bütün məxfi məlumatların müəyyən edildiyini yoxlayın və həssas məlumatlarla necə davranmaq barədə siyasətin mövcud olduğundan əmin olun. ( C8 )

**8.3.5** Əgər məlumat müvafiq məlumatların mühafizəsi üzrə direktivlər əsasında toplanırsa və ya girişin qeydiyyatı tələb olunarsa, məxfi məlumatlara girişin yoxlanıldığını yoxlayın (həssas məlumatların özünü qeyd etmədən).

**8.3.6 Sıfırlardan** və ya təsadüfi məlumatlardan istifadə edərək yaddaşın boşaldılması hücumlarını azaltmaq üçün artıq tələb olunmayan kimi yaddaşda olan həssas məlumatın üzərinə yazıldığını yoxlayın.

**8.3.7 Şifrələnməsi** tələb olunan həssas və ya şəxsi məlumatın həm məxfiliyi, həm də bütövlüyünü təmin edən təsdiq edilmiş alqoritmlərdən istifadə etməklə şifrələndiyini yoxlayın. ( C8 )

**8.3.8** Həssas şəxsi məlumatların məlumat saxlama təsnifatına tabe olduğunu yoxlayın, belə ki, köhnə və ya köhnəlmiş məlumatlar avtomatik olaraq, cədvəl üzrə və ya vəziyyətin tələb etdiyi kimi silinsin.

✓ ✓ ✓ 285 ✓ ✓ ✓ 200 ✓ ✓ 532

✓ ✓ 226

✓ ✓ 327

✓ ✓ 285

Məlumatların qorunmasını nəzərdən keçirərkən, əsas diqqət toplu çıxarılması və ya dəyişdirilməsi və ya həddindən artıq istifadə ətrafında olmalıdır. Məsələn, bir çox sosial media sistemləri istifadəçilərə gündə yalnız 100 yeni dost əlavə etməyə imkan verir, lakin bu sorğuların hansı sistemdən gəldiyi önəmli deyil. Bank platforması xarici təşkilatlara 1000 avrodan çox vəsait köçürməklə saatda 5-dən çox əməliyyatı bloklamaq istəyə bilər. Hər bir sistemin tələbləri çox fərqli ola bilər, ona görə də “anormal” qərar verərkən təhlükə modeli və biznes riski nəzərə alınmalıdır. Əhəmiyyətli meyarlar bu cür anormal toplu hərəkətləri aşkar etmək, qarşısını almaq və ya üstünlük vermək qabiliyyətidir.

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 48



İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• Təhlükəsizlik və anti-keşləmə başlıqlarını yoxlamaq üçün Təhlükəsizlik Başlıqları vebsaytından istifadə etməyi düşünün • OWASP Secure Headers layihəsi

• OWASP Məxfilik Riskləri Layihəsi

• OWASP İstifadəçi Məxfiliyinin Qorunması Fırıldaq Vərəqi

• Avropa İttifaqının Ümumi Məlumatların Qorunması Qaydası (GDPR) icmalı

• Avropa İttifaqının Məlumat Mühafizəsi üzrə Nəzarətçisi - İnternet Məxfilik Mühəndisliyi Şəbəkəsi

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 49



V9 Rabitə

Nəzarət Məqsədi

Təsdiqlənmiş tətbiqin aşağıdakı yüksək səviyyəli tələblərə cavab verdiyinə əmin olun:

• Məzmun həssaslığından asılı olmayaraq TLS və ya güclü şifrələmə tələb edin.

• Ən son təlimatlara əməl edin, o cümlədən:

- Konfiqurasiya məsləhəti

– Üstünlük verilən alqoritmlər və şifrələr

• Son çarə istisna olmaqla, zəif və ya tezliklə köhnələcək alqoritmlərdən və şifrələrdən çəkinin.

Bu tələblər çərçivəsində:

• Təhlükəsiz TLS konfiqurasiyası ilə bağlı tövsiyə olunan sənaye məsləhətlərindən xəbərdar olun, çünki o, tez-tez dəyişir (çox vaxt mövcud alqoritmlərdə və şifrələrdə fəlakətli fasilələr səbəbindən).

• Tercih edilən sıra və alqoritm seçimini konfiqurasiya etmək üçün TLS konfiqurasiyasını nəzərdən keçirmə alətlərinin ən son versiyalarından istifadə edin.

• Təhlükəsiz rabitənin həmişə mövcud və effektiv olmasını təmin etmək üçün vaxtaşırı konfiqurasiyanızı yoxlayın.

V9.1 Müştəri Rabitə Təhlükəsizliyi

TLS 1.2 və ya daha sonrakı versiyalardan istifadə edərək bütün müştəri mesajlarının şifrələnmiş şəbəkələr üzərindən göndərilməsini təmin edin. Müştəri konfiqurasiyasını müntəzəm olaraq nəzərdən keçirmək üçün ən müasir vasitələrdən istifadə edin.

# Təsvir L1 L2 L3 CWE

**9.1.1** TLS-nin bütün müştəri əlaqəsi üçün istifadə edildiyini və təhlükəsiz və ya şifrələnməmiş rabitələrə qayıtmadığını yoxlayın. ( C8 )

**9.1.2** Ən güclü şifrə paketlərinə üstünlük verilməklə, yalnız güclü şifrə dəstlərinin aktiv edildiyini müasir TLS test alətlərindən istifadə edərək yoxlayın.

**9.1.3** TLS protokolunun TLS 1.2 və TLS 1.3 kimi yalnız ən son tövsiyə edilən versiyalarının aktiv edildiyini yoxlayın. TLS protokolunun ən son versiyasına üstünlük verilməlidir.

✓ ✓ ✓ 319 ✓ ✓ ✓ 326 ✓ ✓ ✓ 326

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 50

V9.2 Server Rabitə Təhlükəsizliyi

Server əlaqəsi yalnız HTTP deyil. Monitorinq sistemləri, idarəetmə alətləri, uzaqdan giriş və ssh, ara proqram, verilənlər bazası, əsas çərçivələr, partnyor və ya xarici mənbə sistemləri kimi digər sistemlərə və sistemlərdən təhlükəsiz bağlantılar yerində olmalıdır. Bütün bunlar "xarici cəhətdən çətin, içəridən ələ keçirmək asan" qarşısını almaq üçün şifrələnməlidir.

# Təsvir L1 L2 L3 CWE

**9.2.1** Serverə və serverə qoşulmaların etibarlı TLS sertifikatlarından istifadə etdiyini yoxlayın. Daxili yaradılan və ya öz-özünə imzalanan sertifikatlar istifadə edildikdə, server yalnız xüsusi daxili CA-lara və spesifik özünü imzalanan sertifikatlara etibar etmək üçün konfiqurasiya edilməlidir. Bütün digərləri rədd edilməlidir.

**9.2.2** TLS kimi şifrələnmiş kommunikasiyaların idarəetmə portları, monitorinq, autentifikasiya, API və ya veb xidmət zəngləri, verilənlər bazası, bulud, serversiz,

əsas çərçivə, xarici və partnyor əlaqələri. Server etibarlı olmayan və ya şifrələnməmiş protokollara qayıtmamalıdır.

**9.2.3** Həssas məlumat və ya funksiyaları əhatə edən xarici sistemlərə bütün şifrələnmiş bağlantıların autentifikasiya olunduğunu yoxlayın.

**9.2.4** Onlayn Sertifikat Vəziyyəti Protokolu (OCSP) Stapling kimi düzgün sertifikatın ləğvinin aktiv edildiyini və konfiqurasiya edildiyini yoxlayın.

✓ ✓ 295 ✓ ✓ 319

✓ ✓ 287 ✓ ✓ 299

**9.2.5** Backend TLS əlaqə xətalarının qeyd olunduğunu yoxlayın. ✓ 544

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP – TLS Cheat Sheet

• OWASP - Saxlama Bələdçisi

• “TLS-in təsdiq edilmiş rejimləri” ilə bağlı qeydlər:

– Keçmişdə ASVS ABŞ standartı FIPS 140-2-yə istinad edirdi, lakin qlobal standart kimi ABŞ standartlarını tətbiq etmək çətin, ziddiyyətli və ya çaşdırıcı ola bilər.

– Bölmə 9.1-ə uyğunluğa nail olmaq üçün daha yaxşı üsul Mozilla-nın Server Side TLS kimi bələdçiləri nəzərdən keçirmək və ya məlum yaxşı konfiqurasiyaları yaratmaq və istənilən təhlükəsizlik səviyyəsini əldə etmək üçün məlum və yenilənmiş TLS qiymətləndirmə vasitələrindən istifadə etmək olardı.

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 51

V10 Zərərli Kod

Nəzarət Məqsədi

Kodun aşağıdakı yüksək səviyyəli tələblərə cavab verdiyinə əmin olun:

• Zərərli fəaliyyət tətbiqin qalan hissəsinə təsir etməmək üçün təhlükəsiz və düzgün idarə olunur. • Saatlı bombalar və ya digər vaxta əsaslanan hücumlar yoxdur.

• Zərərli və ya icazəsiz istiqamətlərə "evə zəng etmir".

• Arxa qapıları, Pasxa yumurtaları, salami hücumları, rootkitləri və ya təcavüzkar tərəfindən idarə oluna bilən icazəsiz kodu yoxdur.

Zərərli kodun tapılması neqativin sübutudur, onu tamamilə təsdiqləmək mümkün deyil. Kodun heç bir zərərli kodun və ya arzuolunmaz funksionallığın olmaması üçün ən yaxşı səylər göstərilməlidir.

V10.1 Kodun bütövlüyü

Zərərli koda qarşı ən yaxşı müdafiə "güvən, amma yoxla"dır. Koda icazəsiz və ya zərərli kodun daxil edilməsi çox vaxt bir çox yurisdiksiyalarda cinayət sayılır. Siyasət və prosedurlar zərərli kodla bağlı sanksiyaları aydınlaşdırmalıdır.

Aparıcı tərtibatçılar müntəzəm olaraq kod girişlərini, xüsusən də vaxt, giriş/çıxış və ya şəbəkə funksiyalarına daxil ola bilənləri nəzərdən keçirməlidirlər.

# Təsvir L1 L2 L3 CWE

**10.1.1** Zaman funksiyaları, təhlükəli fayl əməliyyatları və şəbəkə kimi potensial zərərli kodu aşkarlaya bilən kod təhlili alətinin istifadə olunduğunu yoxlayın

əlaqələri.

V10.2 Zərərli Kod Axtarışı

✓ 749

Zərərli kod olduqca nadirdir və onu aşkar etmək çətindir. Əl ilə sətir kodunu nəzərdən keçirmə məntiqi bombaları axtarmağa kömək edə bilər, lakin hətta ən təcrübəli kod nəzərdən keçirən belə, onun mövcud olduğunu bilsələr belə, zərərli kodu tapmaqda çətinlik çəkəcək.

Mənbə koduna, o cümlədən üçüncü tərəfin kitabxanalarına tam giriş olmadan bu bölməyə riayət etmək mümkün deyil.

# Təsvir L1 L2 L3 CWE

**10.2.1** Tətbiqin mənbə kodunun və üçüncü tərəflərin kitabxanalarının icazəsiz ev telefonu və ya məlumat toplama imkanlarının olmadığını yoxlayın. Belə funksionallıq mövcud olduqda, hər hansı məlumat toplamazdan əvvəl onun işləməsi üçün istifadəçinin icazəsini alın.

**10.2.2** Tətbiqin kontaktlar, kameralar, mikrofonlar və ya yer kimi məxfiliklə əlaqəli funksiyalar və ya sensorlar üçün lazımsız və ya həddindən artıq icazə istəmədiyini yoxlayın.

**10.2.3** Tətbiqin mənbə kodunda və üçüncü tərəf kitabxanalarında sərt kodlu və ya əlavə sənədsiz hesablar və ya açarlar, kodun çaşdırılması, sənədsiz binar bloblar, rootkitlər və ya anti-debugging, təhlükəsiz olmayan sazlama xüsusiyyətləri və ya aşkar edilərsə, zərərli məqsədlər üçün istifadə oluna bilən köhnəlmiş, etibarsız və ya gizli funksionallıq.

**10.2.4** Tarix və vaxtla əlaqəli funksiyaları axtararaq proqramın mənbə kodunda və üçüncü tərəf kitabxanalarında saat bombalarının olmadığını yoxlayın.

✓ ✓ 359

✓ ✓ 272 ✓ 507

✓ 511

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 52

# Təsvir L1 L2 L3 CWE

**10.2.5** Tətbiqin mənbə kodunda və üçüncü tərəf kitabxanalarında salam hücumları, məntiqi ötürmələr və ya məntiq bombaları kimi zərərli kodun olmadığını yoxlayın.

**10.2.6** Tətbiqin mənbə kodunda və üçüncü tərəf kitabxanalarında Pasxa yumurtaları və ya hər hansı digər potensial arzuolunmaz funksiyaların olmadığını yoxlayın.

V10.3 Tətbiq bütövlüyü

✓ 511 ✓ 507

Tətbiq yerləşdirildikdən sonra zərərli kod hələ də daxil edilə bilər. Tətbiqlər etibarlı olmayan mənbələrdən imzalanmamış kodun icrası və subdomenlərin ələ keçirilməsi kimi ümumi hücumlardan qorunmalıdır.

Bu bölməyə riayət etmək çox güman ki, operativ və davamlı olacaq.

# Təsvir L1 L2 L3 CWE

**10.3.1 Tətbiqdə** müştəri və ya serverin avtomatik yenilənməsi funksiyası varsa, yeniləmələrin təhlükəsiz kanallar üzərindən əldə edilməli və rəqəmsal imzalanmalı olduğunu yoxlayın. Yeniləmə kodu yeniləməni quraşdırmadan və ya həyata keçirməzdən əvvəl yeniləmənin rəqəmsal imzasını təsdiq etməlidir.

**10.3.2** Tətbiqin kod imzalanması və ya subresurs bütövlüyü kimi bütövlüyün qorunmasından istifadə etdiyini yoxlayın. Tətbiq etibarsız mənbələrdən və ya İnternetdən gələn modullar, plaginlər, kodlar və ya kitabxanaların yüklənməsi kimi etibarsız mənbələrdən kodu yükləməməli və icra etməməlidir.

**10.3.3** Tətbiq müddəti bitmiş domen adları, köhnəlmiş DNS göstəriciləri və ya CNAME-lər, ictimai mənbə kodu repolarında vaxtı keçmiş layihələr və ya keçici bulud API-ləri kimi DNS daxilolmalarına və ya DNS subdomenlərinə əsaslanırsa, tətbiqin subdomenlərin ələ keçirilməsindən qorunduğunu yoxlayın, serversiz funksiyalar və ya saxlama kovaları ( *autogen-bucket-id* .cloud.example.com) və ya oxşar. Mühafizələrə tətbiqlər tərəfindən istifadə edilən DNS adlarının müddətinin bitməsi və ya dəyişdirilməsi üçün müntəzəm olaraq yoxlanılmasının təmin edilməsi daxil ola bilər.

İstinadlar

• Düşmən subdomeninin ələ keçirilməsi, Laboratoriyaları aşkarlayın

• Tərk edilmiş subdomenlərin oğurlanması 2-ci hissə, Detectify Labs

✓ ✓ ✓ 16 ✓ ✓ ✓ 353 ✓ ✓ ✓ 350

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 53

V11 Biznes Məntiqi

Nəzarət Məqsədi

Təsdiqlənmiş tətbiqin aşağıdakı yüksək səviyyəli tələblərə cavab verdiyinə əmin olun:

• Biznes məntiqi axını ardıcıldır, ardıcıllıqla işlənir və yan keçə bilməz.

• Biznes məntiqi avtomatlaşdırılmış hücumları aşkar etmək və qarşısını almaq üçün məhdudiyyətləri ehtiva edir, məsələn, davamlı kiçik pul köçürmələri və ya bir milyon dost əlavə etmək və s.

• Yüksək dəyərli biznes məntiqi axınları sui-istifadə hallarını və zərərli aktorları nəzərdən keçirib və saxtakarlığa, saxtakarlığa, məlumatın açıqlanmasına və imtiyaz hücumlarının artırılmasına qarşı qorunmalara malikdir.

V11.1 Biznes Məntiqi Təhlükəsizliyi

Biznes məntiqi təhlükəsizliyi hər bir tətbiq üçün o qədər fərdidir ki, heç kim yoxlama siyahısı tətbiq etməyəcək. Biznes məntiqi təhlükəsizliyi ehtimal olunan xarici təhdidlərdən qorunmaq üçün nəzərdə tutulmalıdır - onu veb tətbiqi təhlükəsizlik duvarları və ya təhlükəsiz kommunikasiyalardan istifadə etməklə əlavə etmək olmaz. Dizayn sprintləri zamanı təhlükə modelləşdirməsindən istifadə etməyi tövsiyə edirik, məsələn, OWASP Cornucopia və ya oxşar alətlərdən istifadə etməklə.

# Təsvir L1 L2 L3 CWE

**11.1.1** Tətbiqin yalnız eyni istifadəçi üçün biznes məntiqi axınlarını ardıcıl addım sırası ilə və addımları atlamadan emal edəcəyini yoxlayın.

**11.1.2 Tətbiqin** bütün addımların real insan vaxtında emal olunmaqla yalnız biznes məntiqi axınlarını emal edəcəyini, yəni tranzaksiyaların çox tez təqdim edilmədiyini yoxlayın.

**11.1.3 Tətbiqin** hər bir istifadəçi əsasında düzgün tətbiq edilən xüsusi biznes hərəkətləri və ya əməliyyatlar üçün müvafiq məhdudiyyətlərə malik olduğunu yoxlayın.

**11.1.4** Kütləvi məlumatların çıxarılması, biznes məntiqi sorğuları, fayl yükləmələri və ya xidmət hücumlarının rədd edilməsi kimi həddən artıq zənglərdən qorunmaq üçün proqramda anti-avtomatlaşdırma nəzarətlərinə malik olduğunu yoxlayın.

**11.1.5** Tətbiqin təhdid modelləşdirməsi və ya oxşar metodologiyalardan istifadə etməklə müəyyən edilmiş mümkün biznes riskləri və ya təhdidlərindən qorunmaq üçün biznes məntiqi məhdudiyyətlərinə və ya doğrulamaya malik olduğunu yoxlayın.

**11.1.6 Tətbiqin** "İstifadə Vaxtına qədər Yoxlama Vaxtı" (TOCTOU) problemlərindən və ya həssas əməliyyatlar üçün digər yarış şərtlərindən əziyyət çəkmədiyini yoxlayın.

**11.1.7 Tətbiqin** qeyri-adi hadisələrə və ya fəaliyyətə biznes məntiqi baxımından nəzarət etdiyini yoxlayın. Məsələn, nizamsız hərəkətlər və ya normal istifadəçinin heç vaxt cəhd etməyəcəyi hərəkətlər etmək cəhdləri. ( C9 )

**11.1.8** Avtomatlaşdırılmış hücumlar və ya qeyri-adi fəaliyyət aşkar edildikdə proqramın konfiqurasiya edilə bilən xəbərdarlığa malik olduğunu yoxlayın.

✓ ✓ ✓ 841 ✓ ✓ ✓ 799

✓ ✓ ✓ 770 ✓ ✓ ✓ 770

✓ ✓ ✓ 841

✓ ✓ 367

✓ ✓ 754

✓ ✓ 390

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 54

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP Veb Təhlükəsizliyi Testi Bələdçisi 4.1: Biznes Məntiqi Testi

OWASP AppSensor və OWASP -dən istifadə də daxil olmaqla bir çox yolla əldə edilə bilər. Veb Tətbiqlərinə Avtomatlaşdırılmış Təhdidlər

• OWASP AppSensor , həmçinin Hücumun Aşkarlanması və Cavabında kömək edə bilər.

• OWASP Cornucopia

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 55

V12 Fayllar və Resurslar

Nəzarət Məqsədi

Təsdiqlənmiş tətbiqin aşağıdakı yüksək səviyyəli tələblərə cavab verdiyinə əmin olun:

• Etibarsız fayl məlumatları müvafiq qaydada və təhlükəsiz şəkildə işlənməlidir.

• Etibarsız mənbələrdən əldə edilən etibarsız fayl datası veb kökündən kənarda və məhdud icazələrlə saxlanılır.

V12.1 Fayl Yükləmə

Zip bombaları nüfuzetmə testi üsullarından istifadə etməklə ciddi şəkildə sınaqdan keçirilə bilsə də, diqqətlə əllə sınaqdan keçirərək dizayn və inkişafa diqqəti təşviq etmək və xidmətdən imtina vəziyyətinin avtomatlaşdırılmış və ya bacarıqsız əllə nüfuz etmə testindən qaçınmaq üçün L2 və daha yuxarı hesab olunur.

# Təsvir L1 L2 L3 CWE

**12.1.1** Tətbiqin yaddaşı doldura biləcək və ya xidmətdən imtinaya səbəb ola biləcək böyük faylları qəbul etməyəcəyini yoxlayın.

**12.1.2** Tətbiqin sıxılmış faylları (məsələn, zip, gz, docx, odt) maksimum icazə verilən sıxılmamış ölçüyə və faylı sıxışdırmazdan əvvəl faylların maksimum sayına qarşı yoxladığını yoxlayın.

**12.1.3** Bir istifadəçinin yaddaşı həddən artıq çox və ya həddən artıq böyük fayllarla doldura bilməyəcəyinə əmin olmaq üçün hər bir istifadəçi üçün fayl ölçüsü kvotasının və maksimum fayl sayının tətbiq olunduğunu yoxlayın.

V12.2 Fayl bütövlüyü

✓ ✓ ✓ 400 ✓ ✓ 409

✓ ✓ 770

# Təsvir L1 L2 L3 CWE

**12.2.1** Etibarsız mənbələrdən əldə edilmiş faylların faylın məzmununa əsasən gözlənilən tipdə olmasının təsdiqlənməsini yoxlayın.

V12.3 Faylın icrası

✓ ✓ 434

# Təsvir L1 L2 L3 CWE

**12.3.1** İstifadəçi tərəfindən təqdim edilmiş fayl adı metadatasının birbaşa sistem və ya çərçivə fayl sistemləri tərəfindən istifadə edilmədiyini və yol keçidindən qorunmaq üçün URL API-nin istifadə edildiyini yoxlayın.

**12.3.2** Lokal faylların (LFI) açıqlanması, yaradılması, yenilənməsi və ya silinməsinin qarşısını almaq üçün istifadəçi tərəfindən təqdim edilmiş fayl adı metadatasının təsdiq edildiyini və ya nəzərə alınmadığını yoxlayın.

**12.3.3** Uzaqdan Fayl Daxiletmə (RFI) və ya Server tərəfində Sorğu Saxtakarlığı (SSRF) hücumları vasitəsilə uzaq faylların açıqlanmasının və ya icrasının qarşısını almaq üçün istifadəçi tərəfindən təqdim edilmiş fayl adı metadatasının təsdiq edildiyini və ya nəzərə alınmadığını yoxlayın.

**12.3.4** JSON, JSONP və ya URL parametrində istifadəçi tərəfindən təqdim edilmiş fayl adlarını təsdiqləmək və ya məhəl qoymamaqla tətbiqin Yansıtıcı Fayl Yükləməsindən (RFD) qoruduğunu yoxlayın, cavab Məzmun Tipi başlığı mətn/düz olaraq təyin edilməlidir və Məzmun -Disposition başlığının sabit fayl adı olmalıdır.

**12.3.5** ƏS əmrlərinin inyeksiyasından qorunmaq üçün etibarsız fayl metadatasının birbaşa sistem API və ya kitabxanaları ilə istifadə edilmədiyini yoxlayın.

✓ ✓ ✓ 22

✓ ✓ ✓ 73 ✓ ✓ ✓ 98

✓ ✓ ✓ 641 ✓ ✓ ✓ 78

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 56

# Təsvir L1 L2 L3 CWE

**12.3.6 Tətbiqin** təsdiqlənməmiş məzmun paylama şəbəkələri, JavaScript kitabxanaları, node npm kitabxanaları və ya server tərəfi DLL-lər kimi etibarsız mənbələrdən funksionallığı daxil etmədiyini və icra etmədiyini yoxlayın.

V12.4 Fayl Saxlama

✓ ✓ 829

# Təsvir L1 L2 L3 CWE

**12.4.1 Etibarsız** mənbələrdən əldə edilmiş faylların məhdud icazələrlə veb kökündən kənarda saxlandığını yoxlayın.

**12.4.2** Məlum zərərli məzmunun yüklənməsinin və xidmət göstərilməsinin qarşısını almaq üçün etibarsız mənbələrdən əldə edilmiş faylların antivirus skanerləri tərəfindən skan edildiyini yoxlayın.

V12.5 Faylı Endir

✓ ✓ ✓ 552 ✓ ✓ ✓ 509

# Təsvir L1 L2 L3 CWE

**12.5.1 Qəsdən** məlumatın və mənbə kodu sızmasının qarşısını almaq üçün veb səviyyəsinin yalnız xüsusi fayl uzantılarına malik fayllara xidmət etmək üçün konfiqurasiya edildiyini yoxlayın. Məsələn, ehtiyat nüsxə faylları (məsələn, .bak), müvəqqəti işləyən fayllar (məsələn, .swp), sıxılmış fayllar (.zip, .tar.gz və s.) və redaktorlar tərəfindən ümumi istifadə edilən digər genişləndirmələr tələb olunmadığı təqdirdə bloklanmalıdır.

**12.5.2** Yüklənmiş fayllara birbaşa sorğuların heç vaxt HTML/JavaScript məzmunu kimi icra olunmayacağını yoxlayın.

V12.6 SSRF Mühafizəsi

✓ ✓ ✓ 552 ✓ ✓ ✓ 434

# Təsvir L1 L2 L3 CWE

**12.6.1** Veb və ya proqram serverinin serverin sorğu göndərə və ya verilənləri/faylları yükləyə biləcəyi resursların və ya sistemlərin icazə siyahısı ilə konfiqurasiya edildiyini yoxlayın.

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• Həssas Məlumat üçün Fayl Genişləndirilməsi ilə işləmə

• Oren Hafif tərəfindən əks etdirici fayl endirilməsi

• OWASP Üçüncü Tərəf JavaScript İdarəetmə Fırıldaq Vərəqi

✓ ✓ ✓ 918

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 57

V13 API və Veb Xidməti

Nəzarət Məqsədi

Etibarlı xidmət səviyyəsi API-lərindən (adətən JSON və ya XML və ya GraphQL istifadə olunur) istifadə edən təsdiqlənmiş tətbiqin aşağıdakılara malik olduğundan əmin olun:

• Adekvat autentifikasiya, sessiyanın idarə edilməsi və bütün veb xidmətlərinin avtorizasiyası. • Aşağı inam səviyyəsindən yüksək səviyyəyə keçən bütün parametrlərin daxil edilməsinin yoxlanılması. • Bulud və Serversiz API daxil olmaqla, bütün API növləri üçün effektiv təhlükəsizlik nəzarətləri

Zəhmət olmasa, bu fəsli eyni səviyyədə olan bütün digər fəsillərlə birlikdə oxuyun; biz artıq autentifikasiya və ya API sessiyasının idarə edilməsi ilə bağlı narahatlıqları təkrarlamırıq.

V13.1 Ümumi Veb Xidmət Təhlükəsizliyi

# Təsvir L1 L2 L3 CWE

**13.1.1** SSRF və RFI hücumlarında istifadə oluna bilən müxtəlif URI və ya fayl təhlili davranışından istifadə edən təhlil hücumlarının qarşısını almaq üçün bütün proqram komponentlərinin eyni kodlaşdırma və təhliledicilərdən istifadə etdiyini yoxlayın.

**13.1.2** [SİLİNMİŞ, 4.3.1-NİN TƏKRİBİ]

**13.1.3** API URL-lərinin API açarı, sessiya nişanları və s. kimi həssas məlumatları ifşa etmədiyini yoxlayın.

**13.1.4** Avtorizasiya qərarlarının həm URI-də, həm nəzarətçi və ya marşrutlaşdırıcıda proqram təminatı və ya deklarativ təhlükəsizliklə, həm də modelə əsaslanan icazələrlə təmin edilən resurs səviyyəsində qəbul edildiyini yoxlayın.

**13.1.5** Gözlənilməz və ya çatışmayan məzmun növlərini ehtiva edən sorğuların müvafiq başlıqlarla (HTTP cavab statusu 406 Qəbul Edilməz və ya 415 Dəstəklənməyən Media Növü) rədd edildiyini yoxlayın.

V13.2 RESTful Veb Xidməti

✓ ✓ ✓ 116

✓ ✓ ✓ 598 ✓ ✓ 285

✓ ✓ 434

JSON sxeminin yoxlanılması standartlaşdırmanın qaralama mərhələsindədir (istinadlara baxın). RESTful veb xidmətləri üçün ən yaxşı təcrübə olan JSON sxeminin yoxlanılmasından istifadə etməyi nəzərdən keçirərkən, bu əlavə məlumatların doğrulama strategiyalarını JSON sxeminin təsdiqi ilə birlikdə istifadə etməyi düşünün:

• Çatışmayan və ya əlavə elementlərin olması kimi JSON obyektinin təhlilinin yoxlanılması.

• Məlumat növü, məlumat formatı, uzunluq və s. kimi standart daxiletmə yoxlama metodlarından istifadə etməklə JSON obyekti dəyərlərinin doğrulanması.

• və formal JSON sxeminin təsdiqi.

JSON sxeminin təsdiqi standartı rəsmiləşdirildikdən sonra ASVS bu sahədə öz tövsiyələrini yeniləyəcək. İstifadədə olan hər hansı JSON sxeminin doğrulama kitabxanalarını diqqətlə izləyin, çünki standart rəsmiləşdirilənə və istinad tətbiqlərindəki səhvlər aradan qaldırılana qədər onlar müntəzəm olaraq yenilənməlidir.

# Təsvir L1 L2 L3 CWE

**13.2.1** Aktivləşdirilmiş RESTful HTTP metodlarının istifadəçi və ya fəaliyyət üçün düzgün seçim olduğunu yoxlayın, məsələn, normal istifadəçilərin qorunan API və ya resurslarda DELETE və ya PUT istifadəsinin qarşısının alınması.

**13.2.2 Girişi** qəbul etməzdən əvvəl JSON sxeminin təsdiqinin mövcud olduğunu və yoxlanıldığını yoxlayın.

✓ ✓ ✓ 650 ✓ ✓ ✓ 20

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 58

# Təsvir L1 L2 L3 CWE

**13.2.3** Kukilərdən istifadə edən RESTful veb xidmətlərinin aşağıdakılardan ən azı birinin və ya daha çoxunun istifadəsi ilə Saytlararası Sorğu Saxtakarlığından qorunduğunu yoxlayın: kuki nümunəsini iki dəfə təqdim etmək, CSRF qeyri-sətirləri və ya Origin sorğu başlıq yoxlamaları.

**13.2.4** [SİLİNMİŞ, 11.1.4-NİN DUBLİKAT]

**13.2.5** REST xidmətlərinin proqram/xml və ya application/json kimi daxil olan Məzmun Növünün gözlənilən olmasını açıq şəkildə yoxladığını yoxlayın.

**13.2.6** Mesaj başlıqlarının və faydalı yükün etibarlı olduğunu və keçid zamanı dəyişdirilmədiyini yoxlayın. Nəqliyyat üçün güclü şifrələmə tələb etmək (yalnız TLS) bir çox hallarda kifayət ola bilər, çünki bu, həm məxfilik, həm də bütövlüyün qorunmasını təmin edir. Mesaj başına rəqəmsal imzalar yüksək təhlükəsizlik tətbiqləri üçün nəqliyyat mühafizəsi ilə yanaşı əlavə təminat təmin edə bilər, lakin faydaları nəzərə almaq üçün əlavə mürəkkəblik və risklər gətirir.

V13.3 SOAP Veb Xidməti

✓ ✓ ✓ 352

✓ ✓ 436

✓ ✓ 345

# Təsvir L1 L2 L3 CWE

**13.3.1** Düzgün formalaşdırılmış XML sənədini təmin etmək üçün XSD sxeminin yoxlanılmasının baş verdiyini, ardınca həmin məlumatların hər hansı emalından əvvəl hər bir giriş sahəsinin yoxlanılmasını yoxlayın.

**13.3.2** Müştəri və xidmət arasında etibarlı nəqli təmin etmək üçün mesaj yükünün WS-Security istifadə edərək imzalandığını yoxlayın.

✓ ✓ ✓ 20 ✓ ✓ 345

Qeyd: DTD-lərə qarşı XXE hücumları ilə bağlı problemlərə görə, DTD doğrulama istifadə edilməməlidir və V14 Konfiqurasiyasında müəyyən edilmiş tələblərə uyğun olaraq çərçivə DTD qiymətləndirməsi deaktiv edilməlidir.

V13.4 Qrafik QL

# Təsvir L1 L2 L3 CWE

**13.4.1** Bahalı, iç-içə sorğular nəticəsində QraphQL və ya məlumat qatının ifadəsi Xidmətdən imtinanın (DoS) qarşısını almaq üçün sorğuya icazə verilən siyahısının və ya dərinliyin məhdudlaşdırılması və məbləğin məhdudlaşdırılması kombinasiyasının istifadə edildiyini yoxlayın. Daha təkmil ssenarilər üçün sorğu dəyəri analizindən istifadə edilməlidir.

**13.4.2** GraphQL və ya digər məlumat qatının icazə məntiqinin GraphQL qatının əvəzinə biznes məntiqi səviyyəsində həyata keçirilməli olduğunu yoxlayın.

✓ ✓ 770 ✓ ✓ 285

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 59

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP Serversiz Top 10

• OWASP Serversiz Layihəsi

• OWASP Test Bələdçisi 4.0: Konfiqurasiya və Yerləşdirmə İdarəetmə Testi • OWASP Cross-Site Request Forgery fırıldaq vərəqi

• OWASP XML Xarici Müəssisənin Qarşısının Alınması Cheat Sheet - Ümumi Rəhbərlik

• JSON Veb Tokenləri (və İmzalama)

• REST Təhlükəsizlik Fırıldaq Vərəqi

• JSON sxemi

• XML DTD Müəssisə Hücumları

• Orange Tsai - Trend olan Proqramlaşdırma Dillərində SSRF İstifadəsi URL Parserinin yeni dövrü

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 60

V14 Konfiqurasiyası

Nəzarət Məqsədi

Təsdiqlənmiş tətbiqin aşağıdakılara malik olduğundan əmin olun:

• Təhlükəsiz, təkrarlana bilən, avtomatlaşdırıla bilən qurma mühiti.

• Gücləndirilmiş üçüncü tərəf kitabxanası, asılılıq və konfiqurasiya idarəçiliyi, köhnəlmiş və ya etibarsız komponentlər proqrama daxil edilmir.

Tətbiqin qutudan kənar konfiqurasiyası İnternetdə olmaq üçün təhlükəsiz olmalıdır, bu da qutudan kənar konfiqurasiya deməkdir.

V14.1 Yaradın və Yerləşdirin

Quraşdırma boru kəmərləri təkrarlanan təhlükəsizlik üçün əsasdır - hər dəfə təhlükəli bir şey aşkar edildikdə, o, mənbə kodunda həll edilə bilər, qurmaq və ya yerləşdirmə skriptləri və avtomatik sınaqdan keçirilə bilər. Biz istehsala məlum təhlükəsizlik problemlərinin qarşısını almaq üçün tikintini xəbərdar edən və ya pozan avtomatik təhlükəsizlik və asılılıq yoxlanışı ilə tikinti boru kəmərlərinin istifadəsini ciddi şəkildə təşviq edirik. Qeyri-müntəzəm yerinə yetirilən manuel addımlar birbaşa qarşısı alına bilən təhlükəsizlik səhvlərinə gətirib çıxarır.

Sənaye DevSecOps modelinə keçdikcə, “məlum yaxşı” vəziyyətə nail olmaq üçün yerləşdirmə və konfiqurasiyanın davamlı mövcudluğunu və bütövlüyünü təmin etmək vacibdir. Keçmişdə sistem sındırılsaydı, başqa müdaxilənin baş vermədiyini sübut etmək günlər və aylar çəkərdi. Bu gün, proqram təminatı ilə müəyyən edilmiş infrastrukturun, sıfır dayanma vaxtı ilə sürətli A/B yerləşdirmələrinin və avtomatlaşdırılmış konteynerləşdirilmiş quruluşların meydana çıxması ilə hər hansı bir təhlükə altında olan sistem üçün "məlum yaxşı" əvəzetməni avtomatik və davamlı olaraq qurmaq, sərtləşdirmək və yerləşdirmək mümkündür.

Ənənəvi modellər hələ də yerindədirsə, pozulmuş sistemlərin yüksək bütövlükdə, vaxtında güzəştə getməmiş sistemlərlə tez bir zamanda əvəz edilməsinə imkan vermək üçün həmin konfiqurasiyanı sərtləşdirmək və ehtiyat nüsxəsini çıxarmaq üçün əl ilə addımlar atılmalıdır.

Bu bölməyə uyğunluq avtomatlaşdırılmış qurma sistemi və qurmaq və yerləşdirmə skriptlərinə giriş tələb edir. # Təsvir L1 L2 L3 CWE

**14.1.1** Tətbiqlərin qurulması və yerləşdirilməsi proseslərinin CI/CD avtomatlaşdırılması, avtomatlaşdırılmış konfiqurasiya idarəetməsi və avtomatlaşdırılmış yerləşdirmə skriptləri kimi təhlükəsiz və təkrarlana bilən şəkildə yerinə yetirildiyini yoxlayın.

**14.1.2** Kompilyator bayraqlarının bütün mövcud bufer daşması mühafizəsi və xəbərdarlıqlarını, o cümlədən yığının təsadüfiləşdirilməsi, verilənlərin icrasının qarşısının alınması və təhlükəli göstərici, yaddaş, format sətri, tam ədəd və ya sətir əməliyyatları aşkar edildikdə quruluşu pozmaq üçün konfiqurasiya edildiyini yoxlayın.

**14.1.3** Tətbiq serverinin və istifadə olunan çərçivələrin tövsiyələrinə uyğun olaraq server konfiqurasiyasının sərtləşdirildiyini yoxlayın.

**14.1.4** Tətbiq, konfiqurasiya və bütün asılılıqların avtomatlaşdırılmış yerləşdirmə skriptlərindən istifadə etməklə yenidən yerləşdirilə biləcəyini, sənədləşdirilmiş və sınaqdan keçirilmiş runbook-dan ağlabatan müddətdə qurulduğunu və ya ehtiyat nüsxələrdən vaxtında bərpa oluna biləcəyini yoxlayın.

**14.1.5** Təhlükəsizliyi aşkar etmək üçün səlahiyyətli administratorların bütün təhlükəsizliklə əlaqəli konfiqurasiyaların bütövlüyünü yoxlaya biləcəyini yoxlayın.

✓ ✓

✓ ✓ 120

✓ ✓ 16 ✓ ✓

✓

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 61

V14.2 Asılılıq

Asılılığın idarə edilməsi istənilən növ tətbiqin təhlükəsiz işləməsi üçün vacibdir. Köhnəlmiş və ya güvənsiz asılılıqlarla bağlı yeniliklərdən xəbərdar olmamaq bu günə qədər edilən ən böyük və ən bahalı hücumların əsas səbəbidir.

Qeyd: 1-ci Səviyyədə 14.2.1 uyğunluğu daha dəqiq qurulma vaxtı statik kod təhlili və ya asılılıq təhlilindən daha çox müştəri tərəfi və digər kitabxanaların və komponentlərin müşahidələri və ya aşkarlanması ilə əlaqədardır. Bu daha dəqiq üsullar tələb olunduqda müsahibə yolu ilə aşkar edilə bilər.

# Təsvir L1 L2 L3 CWE

**14.2.1** Quraşdırma və ya tərtib müddətində asılılıq yoxlayıcısından istifadə etməklə bütün komponentlərin yeniləndiyini yoxlayın. ( C2 )

**14.2.2** Bütün lazımsız funksiyaların, sənədlərin, nümunə proqramların və konfiqurasiyaların silindiyini yoxlayın.

**14.2.3** Tətbiq aktivləri, məsələn, JavaScript kitabxanaları, CSS və ya veb şriftlər Məzmun Çatdırılma Şəbəkəsində (CDN) və ya xarici provayderdə xaricdə yerləşdirilirsə, aktivin bütövlüyünü yoxlamaq üçün Subresurs Dürüstlüyünün (SRI) istifadə edildiyini yoxlayın.

**14.2.4** Üçüncü tərəf komponentlərinin əvvəlcədən müəyyən edilmiş, etibarlı və davamlı olaraq saxlanılan depolardan gəldiyini yoxlayın. ( C2 )

**14.2.5** İstifadədə olan bütün üçüncü tərəf kitabxanalarının Proqram Təminatı üzrə Materiallar Hesabatının (SBOM) saxlandığını yoxlayın. ( C2 )

**14.2.6 Tətbiqdə** yalnız tələb olunan davranışı üzə çıxarmaq üçün üçüncü tərəf kitabxanalarının qum qutusuna salınması və ya inkapsulyasiya edilməsi ilə hücum səthinin azaldığını yoxlayın. ( C2 )

V14.3 Təhlükəsizliyin nəzərdə tutulmayan açıqlaması

✓ ✓ ✓ 1026 ✓ ✓ ✓ 1002 ✓ ✓ ✓ 829

✓ ✓ 829

✓ ✓

✓ ✓ 265

İstehsal konfiqurasiyaları sazlama konsolları kimi ümumi hücumlardan qorunmaq, Saytlararası Skript (XSS) və Uzaqdan Fayl Daxiletmə (RFI) hücumları üçün zolağı qaldırmaq və arzuolunmaz olan əhəmiyyətsiz informasiya kəşfi "zəifliklərini" aradan qaldırmaq üçün sərtləşdirilməlidir. bir çox nüfuz sınağı hesabatlarının əlamətidir. Bu problemlərin bir çoxu nadir hallarda əhəmiyyətli risk kimi qiymətləndirilir, lakin onlar digər zəifliklərlə birlikdə zəncirlənir. Əgər bu problemlər default olaraq mövcud deyilsə, əksər hücumların uğur qazanmasından əvvəl o, barı qaldırır.

# Təsvir L1 L2 L3 CWE **14.3.1** [SİLİNMİŞ, 7.4.1-İN DUBLİKATI]

**14.3.2** Sazlama xüsusiyyətlərini, inkişaf etdirici konsollarını və gözlənilməz təhlükəsizlik açıqlamalarını aradan qaldırmaq üçün istehsalda veb və ya proqram serverinin və proqram çərçivəsinin debug rejimlərinin söndürüldüyünü yoxlayın.

**14.3.3** HTTP başlıqlarının və ya HTTP cavabının hər hansı hissəsinin sistem komponentlərinin təfərrüatlı versiya məlumatlarını ifşa etmədiyini yoxlayın.

✓ ✓ ✓ 497 ✓ ✓ ✓ 200

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 62

V14.4 HTTP Təhlükəsizlik Başlıqları

# Təsvir L1 L2 L3 CWE

**14.4.1** Hər bir HTTP cavabında Məzmun Tipi başlığı ehtiva etdiyini yoxlayın. Məzmun növləri mətn/\*, /+xml və proqram/xml olarsa, həmçinin təhlükəsiz simvol dəstini (məsələn, UTF-8, ISO-8859-1) təyin edin. Məzmun təqdim edilən Məzmun Növü başlığına uyğun olmalıdır.

**14.4.2** Bütün API cavablarında Content-Disposition: qoşma olduğunu yoxlayın; filename="api.json" başlığı (və ya məzmun növü üçün digər uyğun fayl adı).

**14.4.3** HTML, DOM, JSON və JavaScript inyeksiya zəiflikləri kimi XSS hücumlarının təsirini azaltmağa kömək edən Məzmun Təhlükəsizliyi Siyasətinin (CSP) cavab başlığının mövcud olduğunu yoxlayın.

✓ ✓ ✓ 173

✓ ✓ ✓ 116 ✓ ✓ ✓ 1021

**14.4.4** Bütün cavabların X-Content-Type-Options: nosniff başlığını ehtiva etdiyini yoxlayın. ✓ ✓ ✓ 116

**14.4.5** Strict-Nəqliyyat-Təhlükəsizlik başlığının bütün cavablarda və bütün subdomenlər üçün daxil edildiyini yoxlayın, məsələn, Strict-Nəqliyyat-Təhlükəsizlik: maks.

yaş=15724800; subdomenlər daxildir.

**14.4.6 Etibarsız** tərəflərə Referer başlığı vasitəsilə URL-də həssas məlumatların ifşa edilməsinin qarşısını almaq üçün uyğun Referrer-Siyasət başlığının daxil edildiyini yoxlayın.

**14.4.7** Veb tətbiqinin məzmununun defolt olaraq üçüncü tərəf saytına daxil edilə bilməyəcəyini və dəqiq resursların daxil edilməsinə yalnız uyğun Məzmun-Təhlükəsizlik Siyasəti: çərçivə əcdadları və X-Frame-Seçimlərindən istifadə etməklə zəruri hallarda icazə verildiyini yoxlayın. cavab başlıqları.

V14.5 HTTP Sorğunun Başlığının Təsdiqlənməsi

✓ ✓ ✓ 523 ✓ ✓ ✓ 116 ✓ ✓ ✓ 1021

# Təsvir L1 L2 L3 CWE

**14.5.1** Tətbiq serverinin yalnız proqram/API tərəfindən istifadə edilən HTTP metodlarını, o cümlədən uçuşdan əvvəl OPSİYONLARI qəbul etdiyini və proqram kontekstinə uyğun olmayan istənilən sorğular üzrə qeydləri/xəbərdarlıqları qəbul etdiyini yoxlayın.

**14.5.2** Təchiz edilmiş Origin başlığının autentifikasiya və ya girişə nəzarət qərarları üçün istifadə edilmədiyini yoxlayın, çünki Origin başlığı təcavüzkar tərəfindən asanlıqla dəyişdirilə bilər.

**14.5.3** Mənşə Çarpaz Resurs Paylaşımının (CORS) Giriş-Nəzarət-İcazə Ver Origin başlığının uyğunlaşmaq üçün etibarlı domenlərin və alt domenlərin ciddi icazə siyahısından istifadə etdiyini və "null" mənşəyi dəstəkləmədiyini yoxlayın.

**14.5.4** Etibarlı proksi və ya SSO cihazları tərəfindən əlavə edilmiş HTTP başlıqlarının, məsələn, daşıyıcı tokeninin tətbiq tərəfindən autentifikasiya olunduğunu yoxlayın.

✓ ✓ ✓ 749 ✓ ✓ ✓ 346 ✓ ✓ ✓ 346 ✓ ✓ 306

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 63

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP Veb Təhlükəsizliyi Sınaq Bələdçisi 4.1: HTTP felinin dəyişdirilməsi üçün sınaq

• API cavablarına Content-Disposition əlavə etmək müştəri və server arasında MIME tipində anlaşılmazlığa əsaslanan bir çox hücumların qarşısını almağa kömək edir və "fayl adı" seçimi əks olunanların qarşısını alır. Fayl yükləmə hücumları.

• Məzmun Təhlükəsizliyi Siyasəti Fırıldaq Vərəqi

• BitCoins və Bounties üçün CORS səhv konfiqurasiyasından istifadə

• OWASP Veb Təhlükəsizliyi Testi Bələdçisi 4.1: Konfiqurasiya və Yerləşdirmə İdarəetmə Testi • Sandboxing üçüncü tərəf komponentləri

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 64

Əlavə A: Lüğət

• **Address Space Layout Randomization** (ASLR) – Yaddaşın pozulması ilə bağlı səhvlərdən istifadəni çətinləşdirən texnika.

• **İcazə verin siyahısı** – İcazə verilən məlumatların və ya əməliyyatların siyahısı, məsələn, daxiletmənin yoxlanılmasına icazə verilən simvolların siyahısı.

• **Tətbiq Təhlükəsizliyi** – Tətbiq səviyyəli təhlükəsizlik, məsələn, əsas əməliyyat sistemi və ya qoşulmuş şəbəkələrə diqqət yetirməkdənsə, Açıq Sistemlərin Qarşılıqlı Bağlantı Referans Modelinin (OSI Modeli) tətbiq səviyyəsini təşkil edən komponentlərin təhlilinə diqqət yetirir.

• **Tətbiq Təhlükəsizliyinin Yoxlanması** – OWASP ASVS-ə qarşı tətbiqin texniki qiymətləndirilməsi.

• **Tətbiq Təhlükəsizliyinin Yoxlanması Hesabatı** – Müəyyən tətbiq üçün yoxlayıcı tərəfindən hazırlanmış ümumi nəticələri və dəstəkləyici təhlili sənədləşdirən hesabat.

• **Doğrulama** – Tətbiq istifadəçisinin iddia edilən şəxsiyyətinin yoxlanılması.

• **Avtomatlaşdırılmış Doğrulama** – Problemləri tapmaq üçün zəiflik imzalarından istifadə edən avtomatlaşdırılmış alətlərin (ya dinamik analiz alətləri, statik analiz alətləri və ya hər ikisi) istifadəsi.

• **Qara qutu sınağı** – Bu, proqramın daxili strukturlarına və ya işlərinə nəzər salmadan onun funksionallığını yoxlayan proqram testi üsuludur.

• **Komponent** – digər komponentlərlə əlaqə saxlayan əlaqəli disk və şəbəkə interfeysləri olan müstəqil kod vahidi.

• **Saytlararası** Skript (XSS) – Müştəri tərəfi skriptlərin məzmuna yeridilməsinə imkan verən, adətən veb proqramlarda tapılan təhlükəsizlik zəifliyi.

• **Kriptoqrafik modul** – Kriptoqrafik alqoritmləri həyata keçirən və/yaxud kriptoqrafik açarları yaradan aparat, proqram təminatı və/yaxud proqram təminatı.

• **Ümumi Zəifliklərin Sadalanması** (CWE) - Ümumi proqram təminatının təhlükəsizliyi zəifliklərinin icma tərəfindən hazırlanmış siyahısı. O, ümumi dil, proqram təminatının təhlükəsizliyi alətləri üçün ölçü çubuğu və zəifliklərin müəyyən edilməsi, azaldılması və qarşısının alınması səyləri üçün əsas kimi xidmət edir.

• **Dizayn Doğrulaması** – Tətbiqin təhlükəsizlik arxitekturasının texniki qiymətləndirilməsi.

• **Dinamik Tətbiq Təhlükəsizliyi Testi** (DAST) - Texnologiyalar işlək vəziyyətdə olan proqramda təhlükəsizlik zəifliyini göstərən şərtləri aşkar etmək üçün nəzərdə tutulmuşdur.

• **Dinamik Doğrulama** – Proqramın icrası zamanı problemləri tapmaq üçün zəiflik imzalarından istifadə edən avtomatlaşdırılmış alətlərin istifadəsi.

• **Fast Identity Online** (FIDO) - biometrika, Etibarlı Platforma Modulları (TPM), USB təhlükəsizlik nişanları və s.

• **Qlobal Unikal İdentifikator** (GUID) – proqram təminatında identifikator kimi istifadə edilən unikal istinad nömrəsi.

• **Hyper Text Transfer Protocol** (HTTPS) – Paylanmış, birgə, hipermedia informasiya sistemləri üçün tətbiq protokolu. Bu, Ümumdünya Şəbəkə üçün məlumat kommunikasiyasının əsasını təşkil edir.

• **Sərt kodlu açarlar** – kod, şərh və ya fayllarda olsun, fayl sistemində saxlanılan kriptoqrafik açarlar.

• **Avadanlıq Təhlükəsizliyi Modulu** (HSM) - Kriptoqrafik açarları və digər sirləri qorunan şəkildə saxlamağa qadir olan hardware komponenti.

• **Hibernate Query Language** (HQL) - Hibernate ORM kitabxanası tərəfindən istifadə edilən SQL-ə görünüşünə bənzəyən sorğu dili.

• **Input Validation** – Etibarsız istifadəçi daxiletməsinin kanonikləşdirilməsi və doğrulanması.

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 65



• **Zərərli Kod** – Tətbiqin nəzərdə tutulan təhlükəsizlik siyasətindən yayınan, proqram sahibinin xəbəri olmadan proqramın inkişafı zamanı tətbiqə daxil edilən kod. Virus və ya qurd kimi zərərli proqramlarla eyni deyil!

• **Zərərli proqram** – Proqram istifadəçisi və ya inzibatçısının xəbəri olmadan icra zamanı proqrama daxil edilən icra edilə bilən kod.

• **Açıq Veb Tətbiqinin Təhlükəsizliyi Layihəsi** (OWASP) – Açıq Veb Tətbiqi Təhlükəsizliyi Layihəsi (OWASP) tətbiqi proqram təminatının təhlükəsizliyini təkmilləşdirməyə yönəlmiş dünya üzrə pulsuz və açıq icmadır. Bizim missiyamız tətbiq təhlükəsizliyini "görünən" etməkdir ki, insanlar və təşkilatlar proqram təhlükəsizliyi riskləri haqqında məlumatlı qərarlar qəbul edə bilsinlər. Baxın: https://www.owasp.org/

• **Birdəfəlik Parol** (OTP) - Bir dəfə istifadə edilmək üçün unikal şəkildə yaradılan parol.

• **Obyekt-əlaqəli Xəritəçəkmə** (ORM) - Tətbiqə uyğun olan obyekt modelindən istifadə edərək, tətbiq proqramı çərçivəsində əlaqəli/cədvəl əsaslı verilənlər bazasına istinad etmək və sorğulamaq üçün istifadə olunan sistem.

• **Parol Əsaslı Açar Alma Funksiyası 2** (PBKDF2) - Giriş mətnindən (məsələn, parol) güclü kriptoqrafik açar və əlavə təsadüfi duz dəyəri yaratmaq üçün istifadə edilən xüsusi birtərəfli alqoritmdir və buna görə də istifadə oluna bilər. əldə edilən dəyər orijinal parol əvəzinə saxlanılırsa, parolu oflayn olaraq sındırın.

• **Şəxsi Müəyyənləşdirilə bilən Məlumat** (PII) - tək bir şəxsi müəyyən etmək, əlaqə saxlamaq və ya yerini müəyyən etmək və ya fərdi kontekstdə müəyyən etmək üçün təkbaşına və ya digər məlumatlarla birlikdə istifadə edilə bilən məlumatdır.

• **Position-independent executable** (PIE) - Maşın kodunun gövdəsi, ilkin yaddaşın hardasa yerləşdiyi, mütləq ünvanından asılı olmayaraq düzgün icra olunur.

• **Açıq Açar İnfrastrukturu** (PKI) - Açıq açarları qurumların müvafiq identifikasiyası ilə birləşdirən razılaşma. Məcburiyyət sertifikat orqanında (CA) sertifikatların qeydiyyatı və verilməsi prosesi ilə müəyyən edilir.

• **İctimai Kommutasiyalı Telefon Şəbəkəsi** (PSTN) - Həm stasionar telefonlar, həm də mobil telefonlar daxil olmaqla ənənəvi telefon şəbəkəsi.

• **Etibarlı Tərəf** (RP) - Ümumiyyətlə istifadəçinin ayrıca autentifikasiya provayderinə qarşı autentifikasiyasına əsaslanan proqram. Tətbiq istifadəçinin dedikləri şəxs olduğuna inanmaq üçün həmin identifikasiya provayderi tərəfindən təqdim edilən bir növ işarəyə və ya imzalanmış təsdiqlərə əsaslanır.

• **Static application security testing** (SAST) - Tətbiq mənbə kodunu, bayt kodunu və təhlükəsizlik zəifliklərini göstərən kodlaşdırma və dizayn şərtləri üçün ikili faylları təhlil etmək üçün nəzərdə tutulmuş texnologiyalar toplusu. SAST həlləri işləməyən vəziyyətdə tətbiqi "içdən xaricə" təhlil edir.

• **Proqram təminatının inkişafının həyat dövrü** (SDLC) - Proqram təminatının ilkin tələblərdən tətbiqetmə və texniki xidmətə qədər inkişaf etdirildiyi addım-addım proses.

• **Təhlükəsizlik Arxitekturası** – Təhlükəsizliyə nəzarət vasitələrinin harada və necə istifadə olunduğunu müəyyən edən və təsvir edən, həmçinin həm istifadəçi, həm də proqram məlumatlarının yerini və həssaslığını müəyyən edən və təsvir edən proqram dizaynının abstraksiyasıdır.

• **Təhlükəsizlik Konfiqurasiyası** – Təhlükəsizliyə nəzarətin necə istifadə olunmasına təsir edən proqramın icra vaxtı konfiqurasiyası.

• **Təhlükəsizliyə Nəzarət** – Təhlükəsizlik yoxlanışı (məsələn, girişə nəzarət yoxlaması) həyata keçirən və ya çağırılan zaman təhlükəsizlik effekti ilə nəticələnən (məsələn, audit qeydinin yaradılması) funksiya və ya komponent.

• **Server tərəfində sorğu saxtakarlığı** (SSRF) - Serverdə işləyən kodun məlumatı oxuyacağı və ya təqdim edəcəyi URL-i təmin etmək və ya dəyişdirməklə daxili resursları oxumaq və ya yeniləmək üçün serverin funksionallığından sui-istifadə edən hücum.

• **Single Sign-on Authentication** (SSO) - Bu, istifadəçi bir proqrama daxil olduqda və sonra yenidən autentifikasiya etmədən avtomatik olaraq digər proqramlara daxil olduqda baş verir. Məsələn, Google-a daxil olduqda, YouTube, Google Sənədlər və Gmail kimi digər Google xidmətlərinə daxil olduqda avtomatik olaraq daxil olacaqsınız.

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 66

• **SQL Injection** (SQLi) – Zərərli SQL ifadələrinin giriş nöqtəsinə daxil edildiyi verilənlərə əsaslanan proqramlara hücum etmək üçün istifadə edilən kod yeridilməsi texnikası.

• **SVG** - Ölçəklənən Vektor Qrafikası

• **Zamana əsaslanan OTP** - Cari vaxtın parol yaratmaq üçün alqoritmin bir hissəsi kimi çıxış etdiyi bir OTP yaratmaq üsulu.

• **Təhdidlərin Modelləşdirilməsi** - Təhlükə agentlərini, təhlükəsizlik zonalarını, təhlükəsizlik nəzarətlərini və mühüm texniki və biznes aktivlərini müəyyən etmək üçün getdikcə təkmilləşdirilmiş təhlükəsizlik arxitekturalarının inkişaf etdirilməsindən ibarət texnika.

• **Nəqliyyat Layer Təhlükəsizliyi** (TLS) – Şəbəkə bağlantısı üzərindən rabitə təhlükəsizliyini təmin edən kriptoqrafik protokollar

• **Etibarlı Platforma Modulu** (TPM) - Adətən ana plata kimi daha böyük aparat komponentinə qoşulan və həmin sistem üçün "etibarın kökü" kimi çıxış edən HSM növü.

• **İki faktorlu autentifikasiya** (2FA) - Bu, hesaba giriş üçün identifikasiyanın ikinci səviyyəsini əlavə edir.

• **Universal 2-ci Faktor** (U2F) - USB və ya NFC təhlükəsizlik açarının 2-ci autentifikasiya faktoru kimi istifadəsinə icazə vermək üçün xüsusi olaraq FIDO tərəfindən yaradılmış standartlardan biridir.

• **URI/URL/URL fraqmentləri** – Vahid Resurs İdentifikatoru adı və ya veb resursu müəyyən etmək üçün istifadə olunan simvollar sətridir. Uniform Resource Locator tez-tez mənbəyə istinad kimi istifadə olunur.

• **Doğrulayıcı** – OWASP ASVS tələblərinə uyğun olaraq ərizəni nəzərdən keçirən şəxs və ya komanda.

• **Gördüyünüz** Əldə Etdiyinizdir (WYSIWYG) - Təqdimatı idarə etmək üçün istifadə edilən kodlaşdırmanı göstərməkdənsə, məzmunun təqdim edildikdə necə görünəcəyini göstərən zəngin məzmun redaktoru növü.

• **X.509 Sertifikatı** – X.509 sertifikatı açıq açarın sertifikatda olan istifadəçiyə, kompüterə və ya xidmət identifikasiyasına aid olduğunu yoxlamaq üçün geniş qəbul edilmiş beynəlxalq X.509 açıq açar infrastrukturundan (PKI) istifadə edən rəqəmsal sertifikatdır. .

• **XML eXternal Entity** (XXE) - Elan edilmiş sistem identifikatoru vasitəsilə yerli və ya uzaq məzmuna daxil ola bilən XML obyekti növü. Bu, müxtəlif inyeksiya hücumlarına yüklənə bilər.

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 67

Əlavə B: İstinadlar

Aşağıdakı OWASP layihələri çox güman ki, bu standartın istifadəçiləri/qəbul edənlər üçün faydalıdır: OWASP Əsas Layihələri

1. OWASP Top 10 Layihəsi: https://owasp.org/www-project-top-ten/

2. OWASP Veb Təhlükəsizliyi Test Bələdçisi: https://owasp.org/www-project-web-security-testing-guide/ 3. OWASP Proaktiv Nəzarətlər: https://owasp.org/www-project-proactive-controls/

4. OWASP Təhlükəsizlik Bilik Çərçivəsi: https://owasp.org/www-project-security-knowledge framework/

5. OWASP Software Assurance Maturity Model (SAMM): https://owasp.org/www-project-samm/ OWASP Cheat Sheet Series layihəsi

Bu layihədə ASVS-də müxtəlif mövzular üçün uyğun olacaq bir sıra fırıldaqçı vərəqlər var.

Burada tapıla bilən ASVS üçün xəritə var:

https://cheatsheetseries.owasp.org/cheatsheets/IndexASVS.html

Mobil Təhlükəsizliklə bağlı Layihələr

1. OWASP Mobil Təhlükəsizlik Layihəsi: https://owasp.org/www-project-mobile-security/ 2. OWASP Mobile Top 10 Riskləri: https://owasp.org/www-project-mobile-top-10/

3. OWASP Mobil Təhlükəsizlik Sınaq Bələdçisi və Mobil Tətbiq Təhlükəsizliyi Yoxlama Standartı: https://owasp.org/www-project-mobile-security-testing-guide/

OWASP Əşyaların İnterneti ilə əlaqəli layihələr

1. OWASP Əşyaların İnterneti Layihəsi: https://owasp.org/www-project-internet-of-things/ OWASP Serversiz layihələr

1. OWASP Serversiz Layihəsi: https://owasp.org/www-project-serverless-top-10/ Digərləri

Eynilə, aşağıdakı veb-saytlar bu standartın istifadəçiləri/əbulediciləri üçün çox faydalı ola bilər 1. SecLists Github: https://github.com/danielmiessler/SecLists

2. MITER Ümumi Zəiflik Sadalanması: https://cwe.mitre.org/

3. PCI Təhlükəsizlik Standartları Şurası: https://www.pcisecuritystandards.org

4. PCI Data Security Standard (DSS) v3.2.1 Tələblər və Təhlükəsizlik Qiymətləndirmə Prosedurları: https://www.pcisecuritystandards.org/documents/PCI\_DSS\_v3-2-1.pdf

5. PCI Proqram Təhlükəsizliyi Çərçivəsi - Təhlükəsiz Proqram Tələbləri və Qiymətləndirmə Prosedurları: https://www.pcisecuritystandards.org/documents/PCI-Secure-Software-Standard-v1\_0.pdf

6. PCI Secure Software Lifecycle (Secure SLC) Tələbləri və Qiymətləndirmə Prosedurları: https://www.pcisecuritystandards.org/documents/PCI-Secure-SLC-Standard-v1\_0.pdf

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 68

Əlavə C: Əşyaların İnterneti Doğrulama Tələbləri

Bu fəsil əvvəlcə əsas bölmədə idi, lakin OWASP IoT komandasının gördüyü işlərlə bu mövzuda iki fərqli mövzu saxlamaq mənasızdır. 4.0 buraxılışı üçün biz bunu Əlavəyə köçürürük və bunu tələb edənlərin hamısını əsas OWASP IoT layihəsindən istifadə etməyə çağırırıq.

Nəzarət Məqsədi

Daxili/IoT cihazları:

• Etibarlı mühitdə təhlükəsizlik nəzarətlərini tətbiq etməklə, serverdə olduğu kimi cihaz daxilində təhlükəsizlik nəzarətlərinin eyni səviyyəsinə sahib olun.

• Cihazda saxlanılan həssas məlumatlar təhlükəsiz elementlər kimi hardware tərəfindən dəstəklənən yaddaşdan istifadə etməklə təhlükəsiz şəkildə həyata keçirilməlidir.

• Cihazdan ötürülən bütün həssas məlumatlar nəqliyyat qatının təhlükəsizliyindən istifadə etməlidir. Təhlükəsizlik Yoxlama Tələbləri

# Təsvir L1 L2 L3 ildən

**C.1** Tətbiq səviyyəsinin sazlanması interfeyslərinin, məsələn, USB, UART və digər seriya variantlarının söndürüldüyünü və ya mürəkkəb parolla qorunduğunu yoxlayın.

**C.2** Kriptoqrafik açarların və sertifikatların hər bir fərdi cihaz üçün unikal olduğunu yoxlayın.

**C.3** ASLR və DEP kimi yaddaş mühafizə nəzarətlərinin, əgər varsa, daxil edilmiş/IoT əməliyyat sistemi tərəfindən aktivləşdirildiyini yoxlayın.

**C.4** JTAG və ya SWD kimi çipdə sazlama interfeyslərinin qeyri-aktiv edildiyini və ya mövcud qoruma mexanizminin işə salındığını və müvafiq şəkildə konfiqurasiya edildiyini yoxlayın.

**C.5** Cihaz SoC və ya CPU-da mövcud olduqda, etibarlı icranın həyata keçirildiyini və işə salındığını yoxlayın.

**C.6** Həssas məlumatların, şəxsi açarların və sertifikatların Təhlükəsiz Element, TPM, TEE (Etibarlı İcra Mühiti) içərisində təhlükəsiz şəkildə saxlandığını və ya güclü kriptoqrafiyadan istifadə etməklə qorunduğunu yoxlayın.

**C.7** Mikroproqram proqramlarının nəqliyyat qatının təhlükəsizliyindən istifadə edərək ötürülən məlumatları qoruduğunu yoxlayın.

**C.8** Mikroproqram proqramlarının server bağlantılarının rəqəmsal imzasını təsdiq etdiyini yoxlayın.

✓ ✓ ✓ 4.0 ✓ ✓ ✓ 4.0 ✓ ✓ ✓ 4.0 ✓ ✓ ✓ 4.0 ✓ ✓ ✓ 4.0 ✓ ✓ ✓ 4.0

✓ ✓ ✓ 4.0 ✓ ✓ ✓ 4.0

**C.9** Simsiz rabitənin qarşılıqlı autentifikasiya olunduğunu yoxlayın. ✓ ✓ ✓ 4.0 **C.10** Simsiz rabitənin şifrələnmiş kanal üzərindən göndərilməsini yoxlayın. ✓ ✓ ✓ 4.0

**C.11** Qadağan edilmiş C funksiyalarının hər hansı istifadəsinin müvafiq təhlükəsiz ekvivalent funksiyaları ilə əvəz olunduğunu yoxlayın.

**C.12** Hər bir mikroproqramın üçüncü tərəf komponentlərini, versiyaları və dərc edilmiş zəiflikləri kataloqlaşdıran proqram təminatı sənədlərini saxladığını yoxlayın.

**C.13** Üçüncü tərəf ikili faylları, kitabxanalar, çərçivələr daxil olmaqla bütün kodların sərt kodlaşdırılmış etimadnamələr (arxa qapılar) üçün nəzərdən keçirildiyini yoxlayın.

✓ ✓ ✓ 4.0 ✓ ✓ ✓ 4.0 ✓ ✓ ✓ 4.0

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 69

# Təsvir L1 L2 L3 ildən

**C.14** Qabıq əmr sarğılarını, skriptləri işə salmaqla proqram və mikroproqram komponentlərinin ƏS Əmrlərinin İnyeksiyasına həssas olmadığını yoxlayın və ya təhlükəsizlik nəzarətlərinin ƏS Əmr İnyeksiyasına mane olduğunu yoxlayın.

✓ ✓ ✓ 4.0

**C.15** Mikroproqram proqramlarının rəqəmsal imzanı etibarlı server(lər)ə bağladığını yoxlayın. ✓ ✓ 4.0 **C.16 Müdaxilə** müqavimətinin və/və ya müdaxilənin aşkarlanması xüsusiyyətlərinin mövcudluğunu yoxlayın. ✓ ✓ 4.0

**C.17** Çip istehsalçısı tərəfindən təmin edilən hər hansı mövcud Əqli Mülkiyyətin qorunması texnologiyalarının işə salındığını yoxlayın.

**C.18** Mikroproqramın əks mühəndisliyinə mane olmaq üçün təhlükəsizlik nəzarətlərinin mövcud olduğunu yoxlayın (məsələn, ətraflı sazlama simvollarının çıxarılması).

✓ ✓ 4.0 ✓ ✓ 4.0

**C.19 Yükləmədən** əvvəl cihazın yükləmə şəkli imzasını təsdiq etdiyini yoxlayın. ✓ ✓ 4.0

**C.20** Mikroproqram yeniləmə prosesinin yoxlama vaxtı və istifadə zamanı hücumlarına qarşı həssas olmadığını yoxlayın.

**C.21** Quraşdırmadan əvvəl cihazın kod imzalanmasından istifadə etdiyini və proqram təminatının təkmilləşdirilməsi fayllarını təsdiq etdiyini yoxlayın.

**C.22** Cihazın etibarlı proqram təminatının köhnə versiyalarına endirilə bilməyəcəyini yoxlayın.

**C.23** Daxili cihazda kriptoqrafik cəhətdən təhlükəsiz psevdo-təsadüfi ədəd generatorunun istifadəsini yoxlayın (məsələn, çip tərəfindən təmin edilmiş təsadüfi ədəd generatorlarından istifadə etməklə).

**C.24** Mikroproqramın əvvəlcədən müəyyən edilmiş cədvəl üzrə avtomatik proqram yeniləmələrini həyata keçirə biləcəyini yoxlayın.

**C.25 Təhlükə** aşkar edildikdə və ya etibarsız mesajın alınması zamanı cihazın proqram təminatını və həssas məlumatları sildiyini yoxlayın.

**C.26** Yalnız sazlama interfeyslərinin (məsələn, JTAG, SWD) söndürülməsini dəstəkləyən mikro nəzarətçilərin istifadə edildiyini yoxlayın.

**C.27** Yalnız qapağın açılmasından və yan kanal hücumlarından əhəmiyyətli müdafiəni təmin edən mikro nəzarətçilərin istifadə edildiyini yoxlayın.

**C.28** Həssas izlərin çap dövrə lövhəsinin xarici təbəqələrinə məruz qalmadığını yoxlayın.

**C.29 Çiplərarası rabitənin şifrələndiyini** yoxlayın (məsələn, əsas lövhədən əlavə lövhəyə rabitə).

✓ ✓ 4.0 ✓ ✓ 4.0 ✓ ✓ 4.0 ✓ ✓ 4.0 ✓ ✓ 4.0 ✓ 4.0

✓ 4.0

✓ 4.0

✓ 4.0

✓ 4.0

**C.30** Cihazın kod imzalanmasından istifadə etdiyini və icradan əvvəl kodu təsdiq etdiyini yoxlayın. ✓ 4.0

**C.31 Yaddaşda** saxlanılan həssas məlumatın artıq tələb olunmayan kimi sıfırların üzərinə yazıldığını yoxlayın.

**C.32** Mikroproqram proqramlarının proqramlar arasında izolyasiya üçün nüvə konteynerlərindən istifadə etdiyini yoxlayın.

**C.33** -fPIE, -fstack-protector-all, -Wl,- z,noexecstack, -Wl,-z,noexecheap kimi təhlükəsiz kompilyator bayraqlarının proqram təminatının qurulması üçün konfiqurasiya olunduğunu yoxlayın.

✓ 4.0 ✓ 4.0 ✓ 4.0

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 70

# Təsvir L1 L2 L3 ildən

**C.34** Mikro nəzarətçilərin kod qorunması ilə konfiqurasiya olunduğunu yoxlayın (əgər varsa).

İstinadlar

Əlavə məlumat üçün həmçinin baxın:

• OWASP Əşyaların İnterneti Top 10

• OWASP Daxili Tətbiq Təhlükəsizliyi Layihəsi

• OWASP Əşyaların İnterneti Layihəsi

• Trudy TCP Proksi Aləti

✓ 4.0

OWASP Proqram Təhlükəsizliyi Yoxlama Standartı 4.0.3 71