ECONOMY.GOV.AZ

28 Fevral 2025
TƏHLÜKƏSİZLİK AUDİTİ
Risk: Yüksək

AŞKAR EDİLMİŞ TƏHLÜKƏSİZLİK BOŞLUQLARI / POTENSİAL TƏHLÜKƏSİZLİK PROBLEMLƏRİ / RİSKLƏRİ

1. XSS TƏHLÜKƏSİZLİK BOŞLUQLARI

TAPINTILARIN CİDDİLİK SƏVİYYƏSİ

Aşağıdakı cədvəl, zəiflik və risk təsirini qiymətləndirmək üçün sənəd boyunca istifadə olunan şiddət səviyyələrini və müvafiq CVSS bal aralığını göstərir.

Ciddilik	CVSS V3 bal Aralığı	Tərifi
Çox Yüksək	9.0-10.0	İstismar etmək asandır və adətən sistem səviyyəsində kompromisə səbəb olur.
Yüksək	7.0-8.9	İstismar etmək daha çətindir, lakin yüksəldilmiş səlahiyyətlərə və potensial olaraq məlumat itkisinə və ya iş dayanmasına səbəb ola bilər.
Orta	4.0-6.9	Zəifliklər mövcuddur, lakin istismar edilə bilmir və ya əlavə addımlar, məsələn, sosial mühəndislik tələb edir.
Aşağı	0.1-3.9	Zəifliklər istismar edilə bilmir, lakin qurumun hücum perimetrini azaldır.

Risk Faktorları

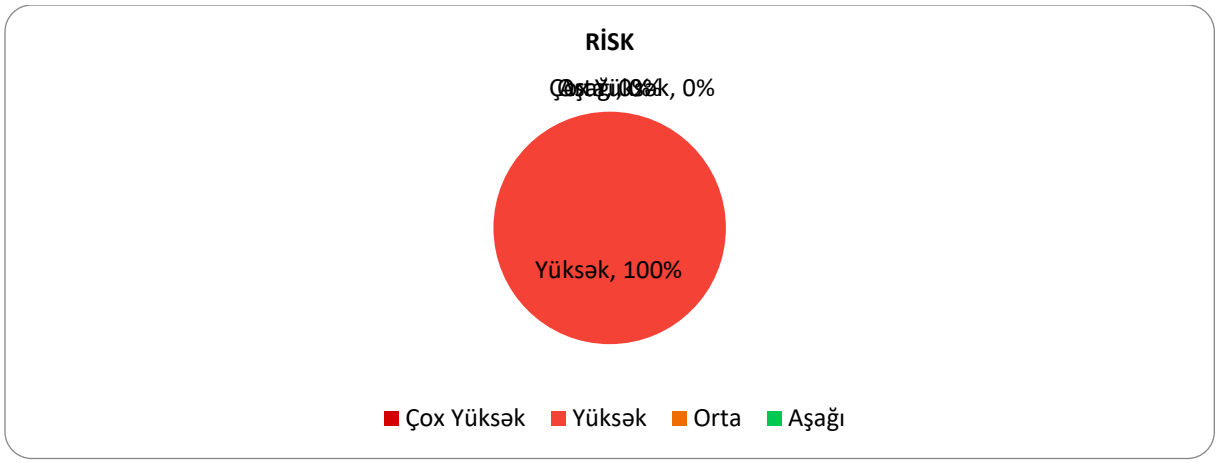
Risk iki faktorla ölçülür: Ehtimal və Təsir.

Ehtimal: Ehtimal zəifliyin istismar edilə bilmə potensialını ölçür. Reytinqlər hücumun çətinliyi, mövcud alətlər və hücumçunun bacarıq səviyyəsi əsasında verilir.

Təsir: Təsir potensial zəifliyin əməliyyatlara təsirini ölçür, o cümlədən qurumun sistemlərinin və ya məlumatlarının məxfiliyi, bütövlüyü və mövcudluğu, reputasiya zərəri və maliyyə itkisi.

AUDİTİN XÜLASƏSİ

RİSK	Çox Yüksək	Yüksək	Orta	Aşağı	TOTAL
	0	1	0	0	1



RİSK	Dərəcəsi
XSS TƏHLÜKƏSİZLİK BOŞLUQLARI	Yüksək

https://economy.gov.az/admin

Risk: Yüksək

1 XSS TƏHLÜKƏSİZLİK BOŞLUQLARI

Admin Panel də "Şəkil" və "Gallery" bölmələrində zərərli skriptlərin yüklənməsi və icrası mümkündür ki, bu da XSS (Cross-Site Scripting) hücumlarına şərait yaradır. Əgər yüklənən fayllar server tərəfində düzgün yoxlanılmırsa, hücumçu zərərli skriptlər, icra edilə bilən fayllar və digər təhlükəli məzmunlar yerləşdirərək sistemə müdaxilə edə bilər.

Məruz URL ünvanlar:

https://economy.gov.az/admin/article/2540/edit?type=news

https://economy.gov.az/admin/article/create?type=news&uniq_id=a4886a70-2145-4595-bed6-7b2077e83aa8

https://economy.gov.az/admin/article/create?type=photogallery&uniq_id=a4886a70-2145-4595-bed6-7b2077e83aa8

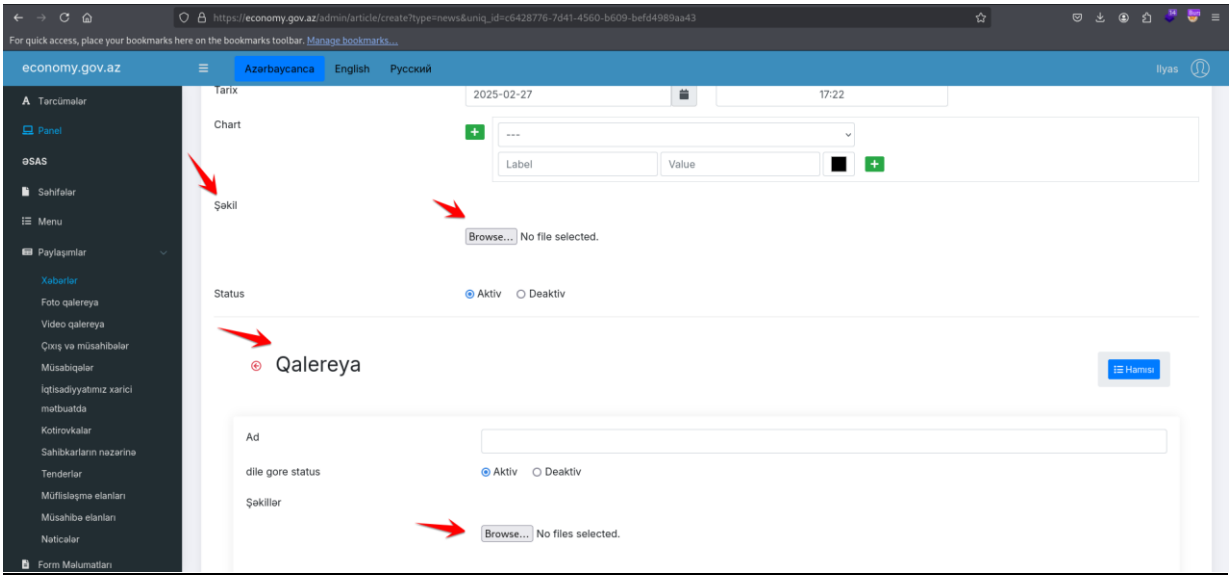
https://economy.gov.az/admin/article/create?type=videogallery&uniq_id=ed40d6d5-eb55-4be1-b168-64dc96682b74

https://economy.gov.az/admin/article/create?type=photogallery&uniq_id=ed40d6d5-eb55-4be1-b168-64dc96682b74

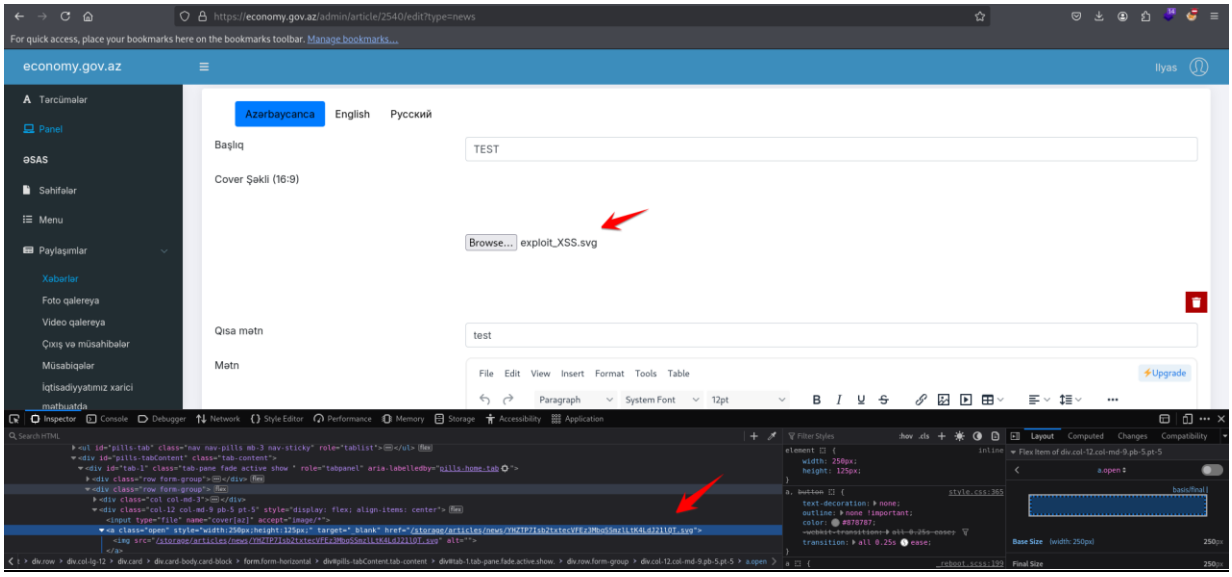
https://economy.gov.az/admin/article/create?type=competitions

https://economy.gov.az/admin/article/create?type=foreign-press&uniq_id=c6428776-7d41-4560-b609-befd4989aa43

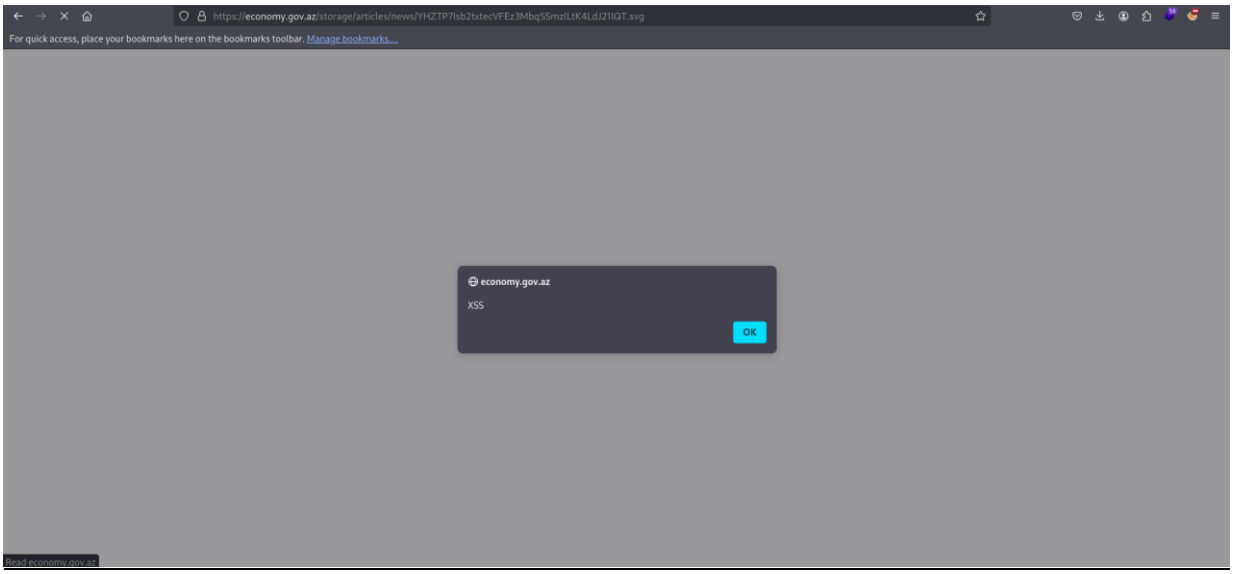
https://economy.gov.az/admin/article/create?type=results&uniq_id=c6428776-7d41-4560-b609-befd4989aa43



Şəkil 1.1. tətbiq edilən bölmələr.



Şəkil 1.2. zərərli faylın yüklənməsi və yerləşməsi. (Xatırladım ki, bu saytın Admin Panel hissəsində "Şəkil" və "Gallery" olan bütün bölmələrində keçərlidir)



Şəkil 1.3. zərərli faylın icra edilməsi. (Xatırladım ki, bu saytın Admin Panel hissəsində "Şəkil" və "Gallery" olan bütün bölmələrində keçərlidir)

HƏLLİ

İstifadəçi tərəfli parametrləri lazımi dərəcədə sanitizə və escape etdikdən sonra istifadəçi brauzerinə “echo” etmək. PHP proqramlaşdırma dilidə aşaqdakı funksiyaların köməyi ilə buna nail ola bilərsiniz:

htmlspecialchars(), urlencode(), strip_tags, htmlententities(), preg_replace() və s.

İstinadlar:

https://grohsfabian.com/xss-through-svg-file-uploads-how-to-fix-with-php/

https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet

https://www.wordfence.com/learn/how-to-prevent-cross-site-scripting-attacks/

http://resources.infosecinstitute.com/how-to-prevent-cross-site-scripting-attacks/

http://php.net/manual/en/function.htmlspecialchars.php

MƏLUMAT XARAKTERLİ QEYDLƏR

1. Trafikin ələ keçirilməsi riskindən sığortalanmaq məqsədilə saytda HTTPS (şifrələnmə imkanlı) protokolundan istifadə edilməsi tövsiyə olunur.

2. Saytda istifadə edilən proqram təminatlarını (CMS, theme, plugin)-lərin, həmçinin server proqram təminatının müxtəlif funksionallıqların daima ən yeni versiyada olmasına diqqət yetirmək və onları vaxtı-vaxtında yeniləmək.

3. Saytın nüsxəsinin hər hansı kənar serverdə saxlanmasına yol verməmək. (istər qurulmuş halda istərsədə arxiv şəklində) Nüsxəni (verilənlər bazası da daxil olmaqla) kənar server(-lər)dən pozmaq.

4. Şifrələr təyin edilərkən (xüsusilə inzibatçı hesablara) unikal və dayanıqlı şifrələrdən istifadə etmək. Şifrələri müntəzəm olaraq dəyişdirmək. Susmaya (default) görə təyin edilmiş şifrələrdən qəti şəkildə istifadə etməmək.

5. Şifrələri, proqram təminatının nüsxələrini elektron poçt ünvanlarında, sosial şəbəkələrdə , müxtəlif bulud (google drive, yandex drive, dropbox və s) kimi kənar resurslarda saxlanmasına qəti şəkildə yol verməmək.

6. Bütün inzibatçı panellərin veb server səviyyəsində (etibarlı IP ünvanlardan və basic avtorizasiyaya) görə qorunmasını təmin etmək tövsiyə edilir.

7. Xidməti məqsədlər üçün yalnız və yalnız müvafiq Dövlət qurumuna / orqanına məxsus mail serverdən istifadə etmək.

8. Sayt üzərində hər hansı funksionallıq dəyişikliyi edərkən təkrar təhlükəsizlik yoxlanışının həyata keçirilməsi məqsədilə bu barədə dərhal məlumat verməyiniz tövsiyə edilir.