

**Р Е П У Б Л И К А Б Ъ Л Г А Р И Я**

**………………………………………**



**ДОКЛАД**

за резултатите от сканиране за уязвимости на информационни ресурси

**Датa:** ………………

Трите имена и длъжността на извършващите сканирането

1. **…………………………………**
2. **………………………….**

**Номер на заповед с която са упълномощени да извършат сканирането: ……………………………..**

**Използвани инструменти**:

* ………………
* ……………….
* ……………….
* …………….
* ……………..
* …………….
* ……………..
* ……………
* ……………….

**ОБЩИ ДАННИ ЗА ИНФОРМАЦИОННИЯ РЕСУРС:**

1. URL: …………………….
2. Засечен IP адрес: …………………
3. Host name: …………………..
4. Domain name: ……………………………………..

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | № на член от НМИМИС/заглавие | № на алинея/точка/подточка и текст на разпоредбата | Въпрос | Отговор | Забележка |
| 1 | Чл. 14/ Филтриране на трафика | (2) Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) трябва да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика. | Засечени ли са отворени ненужни портове по протоколи TCP и User Datagram Protocol (UDP)? |  |  |
| 2 | Чл. 22/ Защита на софтуер и фърмуер | (1) Субектът инсталира и поддържа само версии на използвания в системите му софтуер и фърмуер, които се поддържат от техните доставчици или производители и са актуални от гледна точка на сигурността. | Засечен ли е софтуер, който не отговаря на изискванията на чл. 22 ал. 1? |  |  |
| 3 | Приложение №4 | 9. Да се забрани TLS renegotiation в системи, използващи TLS, или да се конфигурира rate-limiter за ограничаване на броя на предоговаряне на сесия. | Информационният ресурс настроен ли е по начин, по който се забранява TLS renegotiation в системи, използващи TLS, или има конфигуриран ли е rate-limiter за ограничаване на броя на предоговаряне на сесия? |  |  |
| 4 | Приложение №4 | 10. Съобщенията за грешки в системите да не дават излишна информация. | Информационният ресурс настроен ли е по начин, по който се предотвратява предоставяне на излишна информация поради грешки в системата? |  |  |
| 5 | Приложение №4 | 11. Да не се използва AutoComplete. | Засечен ли е AutoComplete? |  |  |
| 6 | Чл. 24/ Защита на уеб сървъри | (1) Субектът предприема следните мерки за защита на уеб сървърите:  1. инсталира сертификат на уеб сървърите си, издаден от доверена система за сертифициране (trusted certification authority system); сертификатът трябва: | Има ли инсталиран сертификат на информационните ресурси, издаден от доверена система за сертифициране (trusted certification authority system)? |  |  |
| 7 | Чл. 24/ Защита на уеб сървъри | а) да е издаден за съответния уеб сайт (website) или група сайтове и да е уникален; | Сертификатът издаден ли е за съответния уеб сайт или група сайтове? |  |  |
| 8 | Чл. 24/ Защита на уеб сървъри |  | Сертификатът уникален ли е? |  |  |
| 9 | Чл. 24/ Защита на уеб сървъри | б) да използва алгоритъм за криптиране поне SHA2; | Сертификатът използва ли алгоритъм за криптиране поне SHA2? |  |  |
| 10 | Чл. 24/ Защита на уеб сървъри | в) да е актуален, като сертификатите с изтекъл срок се анулират; | Сертификатът актуален ли е? |  |  |
| 11 | Чл. 24/ Защита на уеб сървъри |  | Засечени ли са сертификати с изтекъл срок, които не са анулирани? |  |  |
| 12 | Чл. 24/ Защита на уеб сървъри | 2. за защита на интегритета на информацията, обменяна с потребителите, уеб сайтът (website) трябва да е достъпен само по протокол Hypertext Transfer Protocol Secure (HTTPS), като се използват само криптографски транспортни протоколи TLS (Transport Layer Security) версия 1.2, дефиниран в RFC 5246 на IETF (The Internet Engineering Task Force – Специализирана работна група за интернет инженеринг) през 2008 г., версия 1.3, дефиниран в RFC 8446 на IETF през 2018 г., или следващи по-нови версии; | Информационният ресурс достъпен ли е само по протокол Hypertext Transfer Protocol Secure (HTTPS)? |  |  |
| 13 | Чл. 24/ Защита на уеб сървъри |  | В информационния ресурс използват ли се само криптографски транспортни протоколи TLS (Transport Layer Security) версия 1.2, дефиниран в RFC 5246 на IETF (The Internet Engineering Task Force – Специализирана работна група за интернет инженеринг) през 2008 г., версия 1.3, дефиниран в RFC 8446 на IETF през 2018 г., или следващи по-нови версии? |  |  |
| 14 | Чл. 24/ Защита на уеб сървъри | 3. за криптиране на информацията, обменяна между уеб сървъра и потребителите му, се прилагат изискванията на чл. 16 и като се вземат предвид публикуваните в RFC на IETF забрани за използване на методи за шифриране в криптографските транспортни протоколи; | Криптира ли се информацията, обменяна между информационния ресурс и потребителите му? |  |  |
| 15 | Чл. 24/ Защита на уеб сървъри | 5. да не се позволява вмъкване на данни от страна на потребителя, освен на определените за това места; | Засечена ли е възможност за вмъкване на данни от страна на потребителя, освен на определените за това места? |  |  |
| 16 | Чл. 24/ Защита на уеб сървъри | 6. всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя и съдържанието на браузъра, като headеrs на препращащия и потребителски агент, трябва да бъдат валидирани; | Засечена ли е липса на валидация на входните данни, постъпващи от клиента? |  |  |
| 17 | Чл. 24/ Защита на уеб сървъри | 7. приложния софтуер да не позволява въвеждане на специални символи, особено такива, които се използват в SQL заявките; | Засечено ли е дали е възможно да се въвеждат специални символи? |  |  |
| 18 | Чл. 24/ Защита на уеб сървъри | 8. всички данни, изпращани от клиента и показвани в уеб страница, трябва да бъдат кодирани с HTML, за да се гарантира, че съдържанието се изобразява като текст вместо HTML елемент или JavaScript; | Засечени ли са некодирани данни, изпращани от клиента и показвани в уеб страница с HTML? |  |  |
| 19 | Чл. 24/ Защита на уеб сървъри | б) да се конфигурират типът и размерът на headers, които уеб сървърът ще приеме; | Конфигуриран ли е типът и размерът на headers, които информационният ресурс е възможно да приема? |  |  |
| 20 | Чл. 24/ Защита на уеб сървъри | в) да се ограничат времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка, за да се минимизира въздействието и на slow HTTP атаки; | Ограничени ли са времетраенето на връзката (connection Timeout), времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, и минималният брой байтове в секунда при изпращане на отговор на заявка? |  |  |
| 21 | Чл. 24/ Защита на уеб сървъри | 10. за защита от brute force атаки да се въведе ограничение на броя неуспешни опити за влизане в системата; | Засечено ли е ограничение на броя неуспешни опити за влизане в системата? |  |  |
| 22 | Чл. 24/ Защита на уеб сървъри | 11. да не се извежда списък на уеб директориите; | Засечено ли е извеждане на списък на уеб директориите? |  |  |
| 23 | Чл. 24/ Защита на уеб сървъри | 12. бисквитките (cookies) трябва да имат:  а) флаг за защита (security flag) – този флаг инструктира браузъра, че „бисквитката“ може да бъде достъпна само чрез защитени SSL канали; | Имат ли бисквитките (cookies) флаг за защита (security flag)? |  |  |
| 24 | Чл. 24/ Защита на уеб сървъри | б) флаг HTTP only – инструктира браузъра, че „бисквитката“ може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента; | Имат ли бисквитките (cookies) флаг HTTP only? |  |  |
| 25 | Приложение №5 | 1. Headers на отговорите на заявките да не съдържат информация за платформите и версиите на използвания софтуер. | Засечена ли е информация за вида на платформите и версиите на използвания софтуер в Headers на отговорите на заявките? |  |  |
| 26 | Приложение №5 | 2. Headers на отговорите на заявките да съдържат следните опции:  а) HTTP Strict Transport Security (HSTS) – политика съгласно RFC 6797 на IETF от 2012 г., която принуждава уеб браузъра на клиента да се свърже директно чрез HTTPS при преразглеждане на уеб сайта; препоръчителна стойност на периода на валидност на кеша на HSTS (max-age) е поне шест месеца; | Headers на отговорите на заявките съдържат ли опция HTTP Strict Transport Security (HSTS)? |  |  |
| 27 | Приложение №5 | б) X-Content-Type-Options – инструктира потребителския браузър да следва стриктно типа MIME, дефиниран в Content header; единствената валидна стойност за този хедър е „X-Content-Type-Options-nosniff“; | Headers на отговорите на заявките съдържат ли опция X-Content-Type-Options? |  |  |
| 28 | Приложение №5 | в) X-XSS-Protection – настройва конфигурацията за XSS филтъра, вграден в повечето браузъри, което предотвратява някои категории XSS атаки; препоръчителна стойност „X-XSS-Protection: 1; mode=block“; | Headers на отговорите на заявките съдържат ли опция X-XSS-Protection? |  |  |
| 29 | Приложение №5 | г) X-Frame-Options – дава указания на браузъра да не вкарва уеб страницатa във frame/iframe на други уеб страници; препоръчителна стойност „x-frame-options: SAMEORIGIN“; | Headers на отговорите на заявките съдържат ли опция X-Frame-Options? |  |  |
| 30 | Приложение №5 | д) Content-Security-Policy – предотвратява широк спектър от атаки, включително Cross-site scripting и други cross-site injections; | Headers на отговорите на заявките съдържат ли опция Content-Security-Policy? |  |  |
| 31 | Приложение №5 | е) Referrer-Policy Header – позволява на сайта да контролира колко информация с навигация да се включва в браузъра извън документа; | Headers на отговорите на заявките съдържат ли опция Referrer-Policy Header? |  |  |
| 32 | Приложение №5 | ж) Feature-Policy Header – позволява на сайта да контролира кои функции и приложни програмни интерфейси (API) могат да се използват в браузъра; | Headers на отговорите на заявките съдържат ли опция Feature-Policy Header? |  |  |
| 33 | Приложение №5 | з) HTTP Public Key Pinning (HPKP) – защитен механизъм, който позволява на HTTPS уеб сайтовете да се противопоставят на имитация от страна на атакуващите, използвайки неправилно издадени или лъжливи сертификати. | Засечено ли е дали Headers на отговорите на заявките съдържат опция HTTP Public Key Pinning (HPKP)? |  |  |
| 34 | Чл. 24/ Защита на уеб сървъри | 14. в главната директория на уеб сайта (website) да се сложи файл robots.txt, който дава указания на уеб роботите (ботове/паяци) колко често да обхождат сайта, както и кои части от него да обхождат и да индексират; ако този файл не съществува, уеб роботите обхождат целия сайт – всяка една негова страница, подстраница, статия, линк и т.н., което крие риск за конфиденциалността на информацията; | Засечено ли е дали в главната директория на уеб сайта има сложен файл robots.txt? |  |  |
| 35 | Чл. 24/ Защита на уеб сървъри | 15. при използване на Система за управление на съдържанието (CMS) да се промени наименованието по подразбиране на папката за достъп до администраторския панел. | Ако се използва CMS, променено ли е наименованието по подразбиране на папката за достъп до администраторския панел? |  |  |
| 36 | Чл. 25/ Защита на Domain Name System (DNS) | 2. да прилага DNSSEC (Domain Name System Security Extensions); | Засечен ли е DNSSEC? |  |  |
| 37 | Чл. 25/ Защита на Domain Name System (DNS) | 3. да минимизира DNS заявките съгласно RFC 7816 на IETF от 2016 г.; | Минимализирани ли са DNS заявките? |  |  |
| 38 | Чл. 25/ Защита на Domain Name System (DNS) | 4. да забрани zone-transfers – злонамерени лица могат бързо да определят всички хостове в определена зона чрез трансфери на DNS зони, да събират информация за домейна, да избират цели за атаки, да откриват неизползвани IP адреси и да заобикалят мрежовия контрол на достъпа, за да крадат информация; | Засечена ли е забрана на zone-transfers? |  |  |
| 39 | Чл. 25/ Защита на Domain Name System (DNS) | 5. в конфигурационния файл да сложи:  а) dmarc (Domain-based Message Authentication, Reporting and Conformance) запис; | Засечен ли е dmarc (Domain-based Message Authentication, Reporting and Conformance) запис? |  |  |
| 40 | Чл. 25/ Защита на Domain Name System (DNS) | б) SPF (Sender Policy Framework) запис. | Засечен ли е SPF (Sender Policy Framework) запис? |  |  |

**ЗАБЕЛЕЖКА:**

……………………………………………………

**ПРЕПОРЪКИ:**

…………………………………………………..

**Извършили сканирането:**



*Име, фамилия*



*Има, фамилия*