WAS Web Application Report

WAS Default

09 Jun 2026

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

Veljko Vesic
kance_vv

Kancelarije za IT i eUpravu
Save Kova evi a 35b
Kragujevac, None 34000
Serbia

Target and Filters

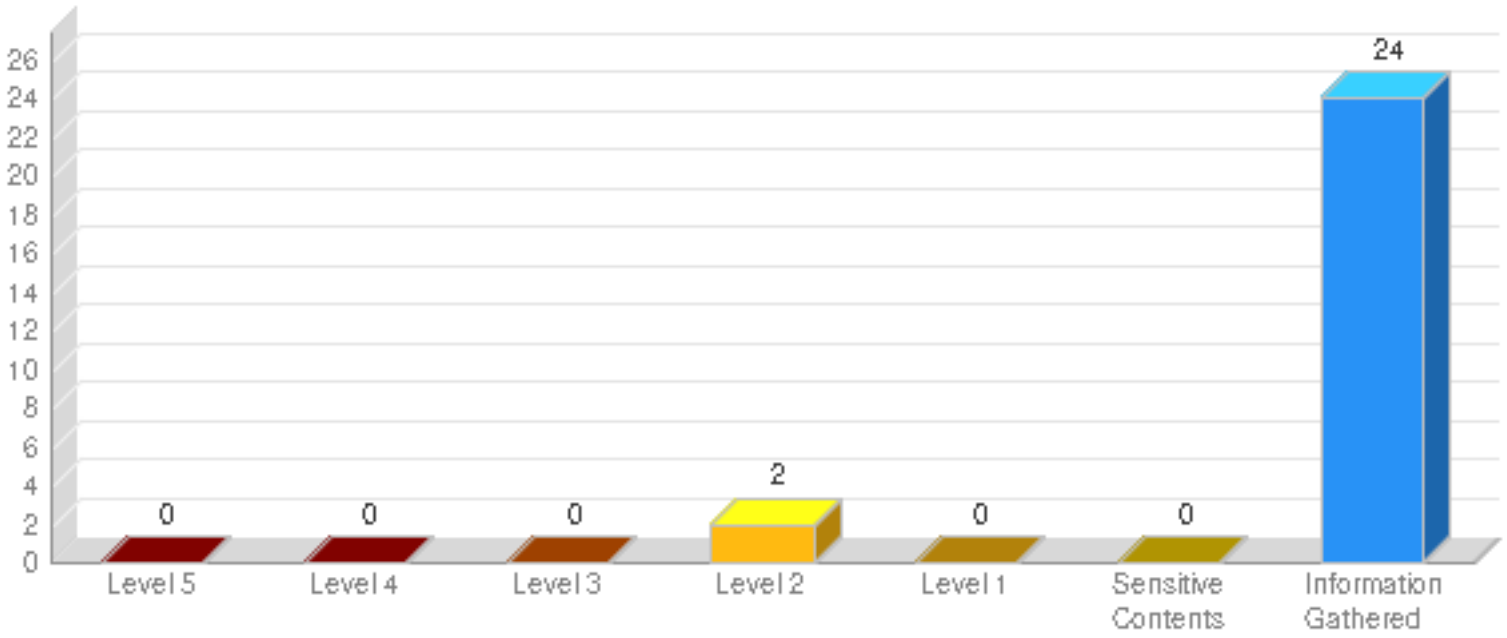
Web Applications (1)	monografije.nitra.gov.rs
Status	New, Active, Re-Opened
Detection Source	Qualys, Burp, Bugcrowd

Summary

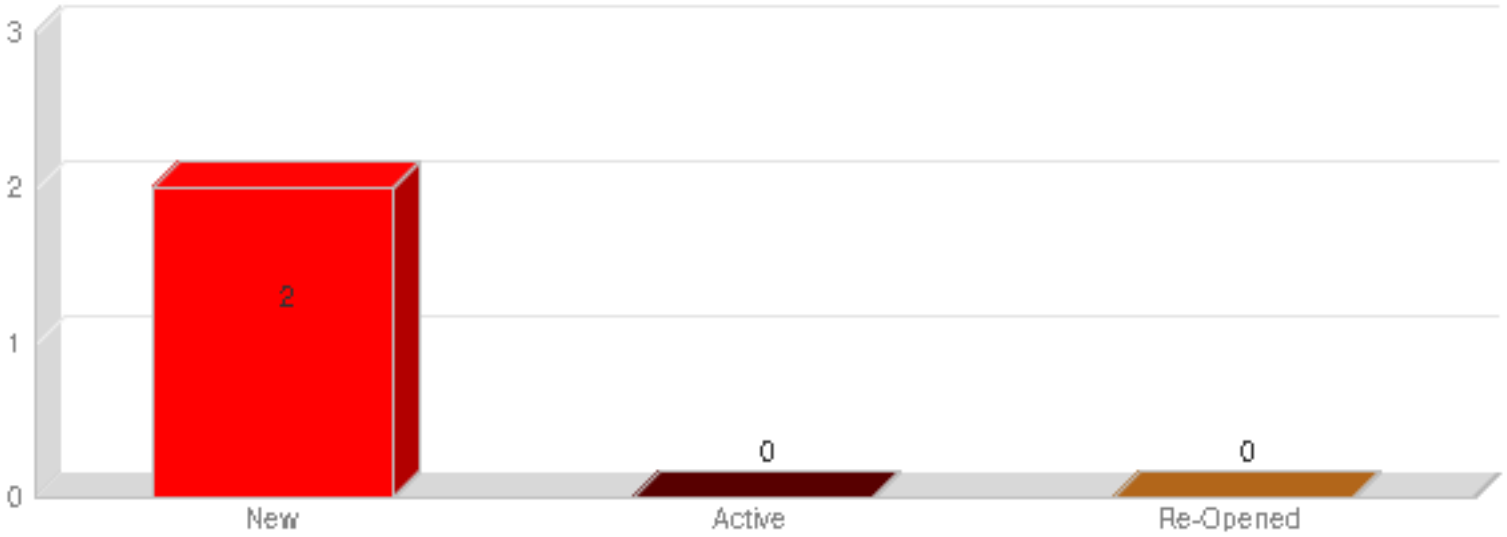
Security Risk	Web Applications	Vulnerabilities	Sensitive Contents	Information Gathered
LOW	1	2	0	24

WAS Web Application Report

Findings by Severity



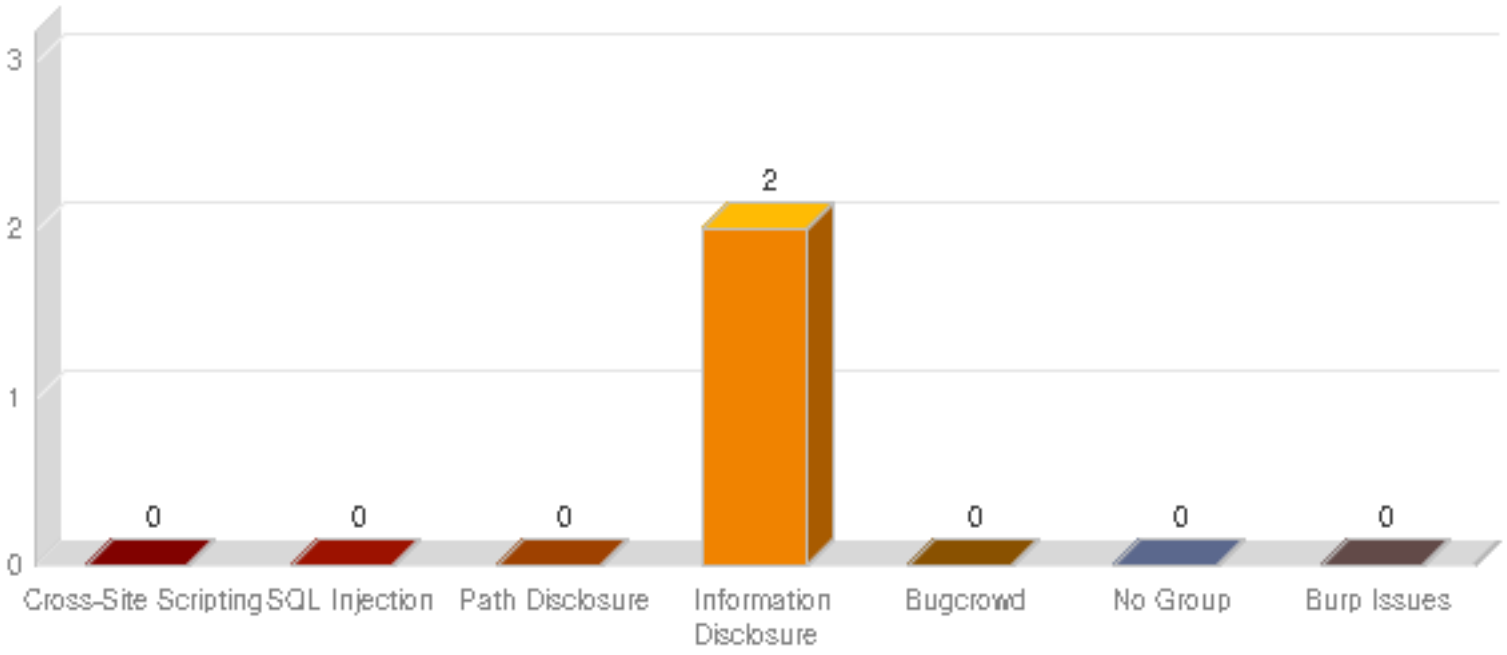
Vulnerabilities by Status



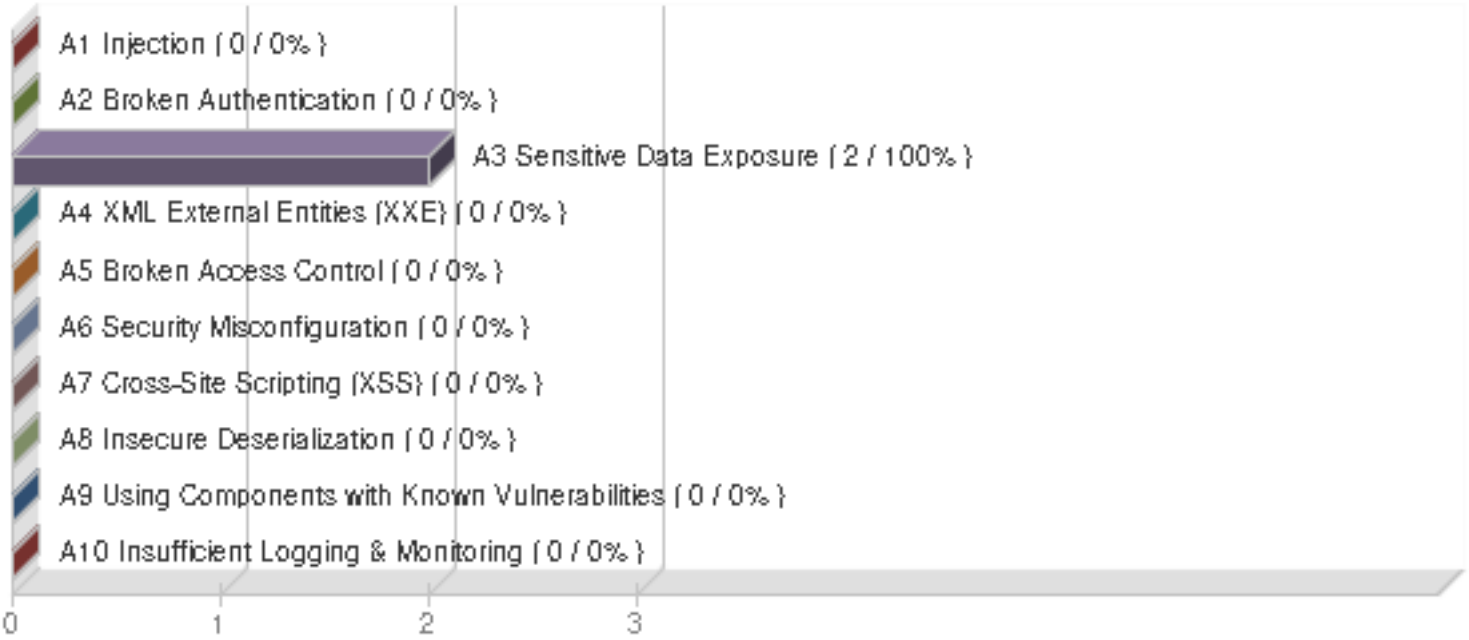
STROGO POVERLJIVO

WAS Web Application Report

Vulnerabilities by Group



OWASP Top 10 2017 Vulnerabilities



Web Application	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
monografije.nitra.gov.rs	0	0	0	2	0	0	24

WAS Web Application Report

Results(26)

Vulnerability (2)

Information Disclosure (2)

150122 Cookie Does Not Contain The "secure" Attribute (1)

https://monografije.nitra.gov.rs/ (1)

150122 Cookie Does Not Contain The "secure" Attribute

monografije.nitra.gov.rs **New**

URL: https://monografije.nitra.gov.rs/

Finding #	198318	**Severity**	Confirmed Vulnerability - Level 2
Unique #	6e90cdca-2c7f-478b-b242-dd382b5eea15		
Group	Information Disclosure	**First Time Detected**	05 Jun 2026 08:03 GMT+0200
CWE	CWE-614	**Last Time Detected**	05 Jun 2026 08:03 GMT+0200
OWASP	A3 Sensitive Data Exposure	**Last Time Tested**	05 Jun 2026 08:03 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	1

CVSS V3 Base 4.3 **CVSS V3 Temporal** 4.1 **CVSS V3 Attack Vector** Network

Details

Threat

The cookie does not contain the "secure" attribute.

Impact

Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

Detection Information

Cookie Name(s) **TS011dbc9d**

Authentication In order to detect this vulnerability, no authentication has been required.

Access Path Here is the path followed by the scanner to reach the exploitable URL:

http://monografije.nitra.gov.rs/

Payloads

WAS Web Application Report

#1 Request

GET https://monografije.nitra.gov.rs/

Host: monografije.nitra.gov.rs
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

TS011dbc9d=
200 OK
Date: Fri, 05 Jun 2026 06:08:00 GMT
Last-Modified: Fri, 07 Apr 2023 11:06:55 GMT
ETag: "0-5f8bd05e8ab18"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; Path=/; Domain=.monografije.nitra.gov.rs

* The reflected string on the response webpage indicates that the vulnerability test was successful

150123 Cookie Does Not Contain The "HTTPOnly" Attribute (1)

https://monografije.nitra.gov.rs/ (1)

150123 Cookie Does Not Contain The "HTTPOnly" Attribute — *monografije.nitra.gov.rs* **New**

URL: https://monografije.nitra.gov.rs/

Finding #	198316	**Severity**	Confirmed Vulnerability - Level 2
Unique #	61fec2a9-c5ec-4328-8470-16058ee17515		
Group	Information Disclosure	**First Time Detected**	05 Jun 2026 08:03 GMT+0200
CWE	CWE-1004	**Last Time Detected**	05 Jun 2026 08:03 GMT+0200
OWASP	A3 Sensitive Data Exposure	**Last Time Tested**	05 Jun 2026 08:03 GMT+0200
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	**Times Detected**	1

CVSS V3 Base 4.3 **CVSS V3 Temporal** 4.1 **CVSS V3 Attack Vector** Network

Details

Threat
The cookie does not contain the "HTTPOnly" attribute.

Impact
Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution
If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

Detection Information

Cookie Name(s) TS011dbc9d

Authentication In order to detect this vulnerability, no authentication has been required.

Access Path Here is the path followed by the scanner to reach the exploitable URL:

http://monografije.nitra.gov.rs/

Payloads

#1 Request

GET https://monografije.nitra.gov.rs/

Host: monografije.nitra.gov.rs
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

TS011dbc9d=
200 OK
Date: Fri, 05 Jun 2026 06:08:00 GMT
Last-Modified: Fri, 07 Apr 2023 11:06:55 GMT
ETag: "0-5f8bd05e8ab18"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; Path=/; Domain=.monografije.nitra.gov.rs

* The reflected string on the response webpage indicates that the vulnerability test was successful

Information Gathered (24)

Scan Diagnostics (17)

150067 Links Discovered During User-Agent and Mobile Site Checks (1)

None (1)

150067 Links Discovered During User-Agent and Mobile Site Checks — *monografije.nitra.gov.r*

Finding #	73870	**Severity**	Information Gathered - Level 3
Unique #	2d5efb68-afa0-4bf3-a0ef-8e012335c479		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Links were discovered via requests using an alternate User-Agent or guessed based on common mobile device URI patterns. The scanner attempts to determine if the Web application changes its behavior when accessed by mobile devices. These checks are based on modifying the User-Agent, changing the domain name, and appending common directories.

The extra links discovered by the Web application scanner during User-Agent manipulation are provided in the Results section.

Impact

The Web application should apply consistent security measures irrespective of browser platform, type or version used to access the application. If the Web application fails to apply security controls to alternate representations of the site, then it may be exposed to vulnerabilities like cross-site scripting, SQL injection, or authorization-based attacks.

Solution

No specific vulnerability has been discovered that requires action to be taken. These links are provided to ensure that a review of the web application includes all possible access points.

Results

Unique content discovered during User-Agent and common mobile device specific subdomains and paths manipulation:

Detected based on: Unique redirect URI
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_2 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7D11 Safari/528.16
URI: http://monografije.nitra.gov.rs/mobile
Redirect URI(302): https://monografije.nitra.gov.rs/mobile

Detected based on: Unique redirect URI
User-Agent: Opera/9.80 (IPhone; Opera Mini/5.0.019802/886; U; en) Presto/2.4.15
URI: http://monografije.nitra.gov.rs/mobile
Redirect URI(302): https://monografije.nitra.gov.rs/mobile

45017 Operating System Detected (1)

None (1)

45017 Operating System Detected

monografije.nitra.gov.r

Finding #	73884	**Severity**	Information Gathered - Level 2
Unique #	77b0fdcd-0a9f-4ea4-a5f0-13652835dbb4		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint**: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS**: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info**: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP**: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

Impact
Not applicable.

Solution
Not applicable.

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	10.2.34.254
Port	-
Result	F5_Big_IP TCP/IP_Fingerprint U7371:443

Info List

Info #1

150009 Links Crawled (1)

None (1)

150009 Links Crawled — *monografije.nitra.gov.r*

Finding #	73873	**Severity**	Information Gathered - Level 1
Unique #	4ab57723-135e-42ae-b497-05a098077f42		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

Impact

N/A

Solution
N/A

Results

Duration of crawl phase (seconds): 319.00
Number of links: 3
(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

https://monografije.nitra.gov.rs/
https://monografije.nitra.gov.rs/.
http://monografije.nitra.gov.rs/

150020 Links Rejected By Crawl Scope or Exclusion List (1)

None (1)

150020 Links Rejected By Crawl Scope or Exclusion List — *monografije.nitra.gov.r*

Finding #	73863	**Severity**	Information Gathered - Level 1
Unique #	60505edf-1d8c-4c92-90a2-d8fcfdcf5c0e		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

Impact
Links listed here were neither crawled or tested by the Web application scanning engine.

Solution
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Results

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

IP based excluded links:

150021 Scan Diagnostics (1)

None (1)

150021 Scan Diagnostics — *monografije.nitra.gov.r*

Finding #	73864	**Severity**	Information Gathered - Level 1
Unique #	99ed725c-c1c3-4b2e-96f7-8eb58f3fefec		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution

No action is required.

Results

Loaded 0 exclude list entries.
Loaded 0 allow list entries.
HTML form authentication unavailable, no WEBAPP entry found
Target web application page http://monografije.nitra.gov.rs/ fetched. Status code:302, Content-Type:, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 1 minute (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 0 seconds. Completed 70 requests of 70 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 59 requests, 1 seconds. Completed 59 requests of 59 estimated requests (100%). All tests completed.
Collected 5 links overall in 0 hours 5 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 3) + paths:(0 x 3) = total (27)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 3 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 18 requests, 0 seconds. Completed 18 requests of 27 estimated requests (66.6667%). All tests completed.
Batch #0 WS enumeration: estimated time < 1 minute (11 tests, 3 inputs)
WS enumeration: 11 vulnsigs tests, completed 23 requests, 0 seconds. Completed 23 requests of 33 estimated requests (69.697%). All tests completed.
Batch #4 WebCgiOob: estimated time < 1 minute (172 tests, 1 inputs)
Batch #4 WebCgiOob: 172 vulnsigs tests, completed 70 requests, 0 seconds. Completed 70 requests of 681 estimated requests (10.279%). All tests completed.
Insufficient Authentication token validation no tests enabled.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 0 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 0 requests, 1 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (38 tests, 0 inputs)
Batch #4 HTTP call manipulation: 38 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (2 tests, 0 inputs)
Batch #4 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 2 seconds. No tests to execute.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 3 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 3 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 1 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 72 requests, 12 seconds. Completed 72 requests of 54 estimated requests (133.333%). XSS optimization removed 87 links. All tests completed.
Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 3 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 484 requests, 14 seconds. Completed 484 requests of 390 estimated requests (124.103%). XSS optimization removed 174 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 3 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 4 requests, 11 seconds. Completed 4 requests of 3 estimated requests (133.333%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(5 x 3) + paths:(10 x 3) = total (45)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 3 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 38 requests, 0 seconds. Completed 38 requests of 45 estimated requests (84.4444%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(1 x 3) + paths:(0 x 3) = total (3)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 3 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 3 estimated requests (66.6667%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(16 x 3) + paths:(0 x 3) = total (48)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 3 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 48 requests, 81 seconds. Completed 48 requests of 48 estimated requests (100%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(1 x 0) + files:(12 x 0) + directories:(147 x 3) + paths:(14 x 3) = total (483)
Batch #5 Path manipulation: estimated time < 1 minute (174 tests, 3 inputs)
Batch #5 Path manipulation: 174 vulnsigs tests, completed 317 requests, 0 seconds. Completed 317 requests of 483 estimated requests (65.6315%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (2223 tests, 1 inputs)
Batch #5 WebCgiGeneric: 2223 vulnsigs tests, completed 1219 requests, 14 seconds. Completed 1219 requests of 11448 estimated requests (10.6481%). All tests completed.
Batch #5 Open Redirect analysis: estimated time < 1 minute (2 tests, 0 inputs)
Batch #5 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 5 seconds. No tests to execute.
Duration of Crawl Time: 319.00 (seconds)
Duration of Test Phase: 405.00 (seconds)
Total Scan Time: 724.00 (seconds)

Total requests made: 2687
Average server response time: 0.01 seconds

Average browser load time: 0.02 seconds

150028 Cookies Collected (1)

None (1)

150028 Cookies Collected

monografije.nitra.gov.r

Finding #	73867	**Severity**	Information Gathered - Level 1
Unique #	fec94286-3f8e-44e9-bc64-2fbcd088368f		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were set by the web application during the crawl phase. This QID will report all the cookies that we detect during the crawl phase, including the excluded cookies. The excluded cookies will be reported since information was gathered, but they will not be tested.

Impact

Cookies may potentially contain sensitive information about the user.

Scan duration may increase if the web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

Solution

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

Results

Total cookies: 1
TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; domain=.monografije.nitra.gov.rs; path=/ First set at URL: https://monografije.nitra.gov.rs/

150546 First Link Crawled Response Code Information (1)

None (1)

150546 First Link Crawled Response Code Information — *monografije.nitra.gov.r*

Finding #	73869	**Severity**	Information Gathered - Level 1
Unique #	8164ed37-ca46-470f-8628-94ac5d671310		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

Impact

An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

Solution

Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

Results

Base URI: http://monografije.nitra.gov.rs/
Response Code: 302
Response Header:
Location: https://monografije.nitra.gov.rs/
Server: BigIP
Connection: Keep-Alive
Content-Length: 0
Set-Cookie: TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; domain=.monografije.nitra.gov.rs; path=/

Response Body:

38116 SSL Server Information Retrieval (1)

None (1)

38116 SSL Server Information Retrieval — *monografije.nitra.gov.r*

Finding #	73882	**Severity**	Information Gathered - Level 1
Unique #	1b516776-73d0-4589-b2fb-69386dba8e7f		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	monografije.nitra.gov.rs
IP	10.2.34.254
Port	443
Result	#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1 COMPRESSION_METHOD None _ _ _ AES128-SHA RSA R SHA1 AES(128) MEDIUM DHE-RSA-AES128-SHA DH RSA SHA1 AES(128) MEDIUM AES256-SHA RSA RSA SHA1 AES(256) HIGH DHE-RSA-AES256-SHA RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM DHE-RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIU CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(256) HIGH ECDHE-RSA-AES128-SHA ECD RSA SHA1 AES(128) MEDIUM ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH TLSv1.1_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.1 COMPRESSION_METHOD None _ _ _ AES128-SHA RSA RSA SHA1 AES(128) MEDIUM DHE-RSA-AES128-SHA DH RSA SHA1 AES(128) MEDIUM AES25 SHA RSA RSA SHA1 AES(256) HIGH DHE-RSA-AES256-SHA DH RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM D RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIUM CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(256) HIGH ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HI TLSv1.2_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.2 COMPRESSION_METHOD None _ _ _ AES128-SHA RSA RSA SHA1 AES(128) MEDIUM DHE-RSA-AES128-SHA DH RSA SHA1 AES(128) MEDIUM AES256-SHA RSA RSA SHA1 AES(256) HIGH DHE-RSA-AES256-SHA DH RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM DHE-RSA-AES128-SHA2 DH RSA SHA256 AES(128) MEDIUM DHE-RSA-AES256-SHA256 DH RSA SHA256 AES(256) HIGH CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(256) HIGH AES128-GCM-SHA256 RSA RSA AEAD AESGCM(128) MEDIUM AES256-GCM-SHA384 R RSA AEAD AESGCM(256) HIGH DHE-RSA-AES128-GCM-SHA256 DH RSA AEAD AESGCM(128) MEDIUM DHE-RSA-AES256-GCM-SHA384 DH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH ECDHE RSA-AES128-SHA256 ECDH RSA SHA256 AES(128) MEDIUM ECDHE-RSA-AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH ECDHE-RSA-AES128-G SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH AES128-SHA256 RSA RSA SHA256 AES(128) MEDIUM AES256-SHA256 RSA RSA SHA256 AES(256) HIGH TLSv1.3_PROTOCOL_IS_DISABLED _ _ _ _ _

Info List

Info #1

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
AES128-SHA	RSA	AES(128)	MEDIUM	RSA	SHA1	TLSv1
AES128-SHA	RSA	AES(128)	MEDIUM	DH	SHA1	TLSv1
AES128-SHA	RSA	AES(256)	HIGH	RSA	SHA1	TLSv1
AES128-SHA	RSA	AES(256)	HIGH	DH	SHA1	TLSv1
AES128-SHA	RSA	Camellia(128)	MEDIUM	RSA	SHA1	TLSv1
AES128-SHA	RSA	Camellia(128)	MEDIUM	DH	SHA1	TLSv1
AES128-SHA	RSA	Camellia(256)	HIGH	RSA	SHA1	TLSv1
AES128-SHA	RSA	Camellia(256)	HIGH	DH	SHA1	TLSv1
AES128-SHA	RSA	AES(128)	MEDIUM	ECDH	SHA1	TLSv1
AES128-SHA	RSA	AES(256)	HIGH	ECDH	SHA1	TLSv1

Info #2

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
AES128-SHA	RSA	AES(128)	MEDIUM	RSA	SHA1	TLSv1.1
AES128-SHA	RSA	AES(128)	MEDIUM	DH	SHA1	TLSv1.1
AES128-SHA	RSA	AES(256)	HIGH	RSA	SHA1	TLSv1.1
AES128-SHA	RSA	AES(256)	HIGH	DH	SHA1	TLSv1.1
AES128-SHA	RSA	Camellia(128)	MEDIUM	RSA	SHA1	TLSv1.1
AES128-SHA	RSA	Camellia(128)	MEDIUM	DH	SHA1	TLSv1.1
AES128-SHA	RSA	Camellia(256)	HIGH	RSA	SHA1	TLSv1.1
AES128-SHA	RSA	Camellia(256)	HIGH	DH	SHA1	TLSv1.1
AES128-SHA	RSA	AES(128)	MEDIUM	ECDH	SHA1	TLSv1.1
AES128-SHA	RSA	AES(256)	HIGH	ECDH	SHA1	TLSv1.1

Info #3

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	ECDH	AEAD	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(128)	MEDIUM	RSA	SHA256	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(256)	HIGH	RSA	SHA256	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(128)	MEDIUM	RSA	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(128)	MEDIUM	DH	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(256)	HIGH	RSA	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(256)	HIGH	DH	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	Camellia(128)	MEDIUM	RSA	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	Camellia(128)	MEDIUM	DH	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(128)	MEDIUM	DH	SHA256	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(256)	HIGH	DH	SHA256	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	Camellia(256)	HIGH	RSA	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	Camellia(256)	HIGH	DH	SHA1	TLSv1.2

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(128)	MEDIUM	RSA	AEAD	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	RSA	AEAD	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(128)	MEDIUM	DH	AEAD	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	DH	AEAD	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(128)	MEDIUM	ECDH	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(256)	HIGH	ECDH	SHA1	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(128)	MEDIUM	ECDH	SHA256	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AES(256)	HIGH	ECDH	SHA384	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(128)	MEDIUM	ECDH	AEAD	TLSv1.2

38291 SSL Session Caching Information (1)

None (1)

38291 SSL Session Caching Information — *monografije.nitra.gov.r*

Finding #	73878	**Severity**	Information Gathered - Level 1
Unique #	8881dd0c-1a97-415a-bee3-8503e852f958		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

Impact
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	monografije.nitra.gov.rs
IP	10.2.34.254
Port	443
Result	TLSv1 session caching is enabled on the target. TLSv1.1 session caching is enabled on the target. TLSv1.2 session caching is enabled on the target.

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (1)

None (1)

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance — *monografije.nitra.gov.r*

Finding #	73880	**Severity**	Information Gathered - Level 1
Unique #	8021cadd-09de-427d-8abd-4709bf03706b		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	monografije.nitra.gov.rs
IP	10.2.34.254
Port	443

Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

38609 SSL Server default Diffie-Hellman prime information (1)

None (1)

38609 SSL Server default Diffie-Hellman prime information — *monografije.nitra.gov.r*

Finding #	73881	**Severity**	Information Gathered - Level 1
Unique #	915fd00d-3660-47df-a5d7-2f0f613490fe		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS. - For fixed primes: 1024 and below are considered unsafe. - For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	monografije.nitra.gov.rs
IP	10.2.34.254
Port	443
Result	SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (1)

None (1)

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — *monografije.nitra.gov.r*

Finding #	73883	**Severity**	Information Gathered - Level 1
Unique #	e657d318-49c5-41f1-9971-00d31c1b46d0		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	monografije.nitra.gov.rs
IP	10.2.34.254
Port	443
Result	#table cols="7" CIPHER NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1 _ _ _ _ _ _ CAMELLIA256-S RSA _ 4096 no 150 low CAMELLIA128-SHA RSA _ 4096 no 150 low AES256-SHA RSA _ 4096 no 150 low AES128-SHA RSA _ 4096 no 150 low DHE-RSA-CAMELLIA256-SHA DHE _ 2048 yes 110 low DHE-RSA-CAMELLIA256-SHA DHE _ 3072 yes 132 low DHE-RSA-CAMELLIA256-SHA DHE _ 4096 yes 150 low DHE-RSA-CAMELLIA128-SHA DHE _ 2048 yes 110 low DHE-RSA-CAMELLIA128-SHA DHE _ 3072 yes 132 low DHE-RSA-CAMELLIA128-SHA DHE _ 4096 y 150 low DHE-RSA-AES256-SHA DHE _ 2048 yes 110 low DHE-RSA-AES256-SHA DHE _ 3072 yes 132 low DHE-RSA-AES256-SHA DHE _ 4096 yes 150 low DHE-RSA-AES128-SHA DHE _ 2048 yes 110 low DHE-RSA-AES128-SHA DHE _ 3072 yes 132 low DHE-RSA-AES128-SHA DHE _ 4096 yes 150 low ECDHE-RSA-AES256-SHA ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES256-SHA ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES256-SHA ECDHE x25519 256 yes 128 low ECDHE-RSA-AES128-SHA ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES128-SHA ECDHE secp256r1 256 yes 128 low ECDH RSA-AES128-SHA ECDHE x25519 256 yes 128 low TLSv1.1 _ _ _ _ _ _ CAMELLIA256-SHA RSA _ 4096 no 150 low CAMELLIA128-SHA RSA _ 4096 no 150 AES256-SHA RSA _ 4096 no 150 low AES128-SHA RSA _ 4096 no 150 low DHE-RSA-CAMELLIA256-SHA DHE _ 2048 yes 110 low DHE-RSA-CAMELLIA256 SHA DHE _ 3072 yes 132 low DHE-RSA-CAMELLIA256-SHA DHE _ 4096 yes 150 low DHE-RSA-CAMELLIA128-SHA DHE _ 2048 yes 110 low DHE-RSA-CAMELLIA128-SHA DHE _ 3072 yes 132 low DHE-RSA-CAMELLIA128-SHA DHE _ 4096 yes 150 low DHE-RSA-AES256-SHA DHE _ 2048 yes 110 low DHE-RSA-AES256-SHA DHE _ 3072 yes 132 low DHE-RSA-AES256-SHA DHE _ 4096 yes 150 low DHE-RSA-AES128-SHA DHE _ 2048 yes 110 low DHE-RSA-AES128 SHA DHE _ 3072 yes 132 low DHE-RSA-AES128-SHA DHE _ 4096 yes 150 low ECDHE-RSA-AES256-SHA ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES256-SHA ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES256-SHA ECDHE x25519 256 yes 128 low ECDHE-RSA-AES128-SHA ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES128-SHA ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES128-SHA ECDHE x25519 256 yes 128 low TLSv1.2 _ _ _ _ _ _ AES256-SHA256 RSA _ 4096 no 150 low AES128-SHA256 RSA _ 4096 no 150 low AES256-GCM-SHA384 RSA _ 4096 no 150 low AES128-GCM-SHA256 RS 4096 no 150 low CAMELLIA256-SHA RSA _ 4096 no 150 low CAMELLIA128-SHA RSA _ 4096 no 150 low AES256-SHA RSA _ 4096 no 150 low AES128-SHA RSA _ 4096 no 150 low DHE-RSA-AES256-GCM-SHA384 DHE _ 2048 yes 110 low DHE-RSA-AES256-GCM-SHA384 DHE _ 3072 yes 132 low DHE-RSA-AES GCM-SHA384 DHE _ 4096 yes 150 low DHE-RSA-AES128-GCM-SHA256 DHE _ 2048 yes 110 low DHE-RSA-AES128-GCM-SHA256 DHE _ 3072 yes 132 low DHE-RSA-AES128-GCM-SHA256 DHE _ 4096 yes 150 low DHE-RSA-AES256-SHA256 DHE _ 2048 yes 110 low DHE-RSA-AES256-SHA256 DHE _ 3072 yes low DHE-RSA-AES256-SHA256 DHE _ 4096 yes 150 low DHE-RSA-CAMELLIA256-SHA DHE _ 2048 yes 110 low DHE-RSA-CAMELLIA256-SHA DHE _ 3072 132 low DHE-RSA-CAMELLIA256-SHA DHE _ 4096 yes 150 low DHE-RSA-AES128-SHA256 DHE _ 2048 yes 110 low DHE-RSA-AES128-SHA256 DHE _ 307 yes 132 low DHE-RSA-AES128-SHA256 DHE _ 4096 yes 150 low DHE-RSA-CAMELLIA128-SHA DHE _ 2048 yes 110 low DHE-RSA-CAMELLIA128-SHA DHE 3072 yes 132 low DHE-RSA-CAMELLIA128-SHA DHE _ 4096 yes 150 low DHE-RSA-AES256-SHA DHE _ 2048 yes 110 low DHE-RSA-AES256-SHA DHE _ 3(yes 132 low DHE-RSA-AES256-SHA DHE _ 4096 yes 150 low DHE-RSA-AES128-SHA DHE _ 2048 yes 110 low DHE-RSA-AES128-SHA DHE _ 3072 yes 132 DHE-RSA-AES128-SHA DHE _ 4096 yes 150 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES256-GCM-SHA3 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE x25519 256 yes 128 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE x25519 25 yes 128 low ECDHE-RSA-AES256-SHA384 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES256-SHA384 ECDHE secp256r1 256 yes 128 low ECDHE-R AES256-SHA384 ECDHE x25519 256 yes 128 low ECDHE-RSA-AES128-SHA256 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES128-SHA256 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES128-SHA256 ECDHE x25519 256 yes 128 low ECDHE-RSA-AES256-SHA ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES256-SHA ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES256-SHA ECDHE x25519 256 yes 128 low ECDHE-RSA-AES128-SHA ECDH secp384r1 384 yes 192 low ECDHE-RSA-AES128-SHA ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES128-SHA ECDHE x25519 256 yes 128 low

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size		Classical	Quantum
RSA		TLSv1	4096	no	150	low
RSA		TLSv1	4096	no	150	low
RSA		TLSv1	4096	no	150	low
RSA		TLSv1	4096	no	150	low
DHE		TLSv1	2048	yes	110	low
DHE		TLSv1	3072	yes	132	low
DHE		TLSv1	4096	yes	150	low
DHE		TLSv1	2048	yes	110	low
DHE		TLSv1	3072	yes	132	low
DHE		TLSv1	4096	yes	150	low
DHE		TLSv1	2048	yes	110	low
DHE		TLSv1	3072	yes	132	low
DHE		TLSv1	4096	yes	150	low
DHE		TLSv1	2048	yes	110	low
DHE		TLSv1	3072	yes	132	low
DHE		TLSv1	4096	yes	150	low
ECDHE		TLSv1	384	yes	192	low
ECDHE		TLSv1	256	yes	128	low
ECDHE		TLSv1	256	yes	128	low
ECDHE		TLSv1	384	yes	192	low
ECDHE		TLSv1	256	yes	128	low
ECDHE		TLSv1	256	yes	128	low
RSA		TLSv1.1	4096	no	150	low
RSA		TLSv1.1	4096	no	150	low
RSA		TLSv1.1	4096	no	150	low
RSA		TLSv1.1	4096	no	150	low
DHE		TLSv1.1	2048	yes	110	low
DHE		TLSv1.1	3072	yes	132	low
DHE		TLSv1.1	4096	yes	150	low
DHE		TLSv1.1	2048	yes	110	low

Kex	Group	Protocol	Key Size		Classical	Quantum
DHE		TLSv1.1	3072	yes	132	low
DHE		TLSv1.1	4096	yes	150	low
DHE		TLSv1.1	2048	yes	110	low
DHE		TLSv1.1	3072	yes	132	low
DHE		TLSv1.1	4096	yes	150	low
DHE		TLSv1.1	2048	yes	110	low
DHE		TLSv1.1	3072	yes	132	low
DHE		TLSv1.1	4096	yes	150	low
ECDHE		TLSv1.1	384	yes	192	low
ECDHE		TLSv1.1	256	yes	128	low

Kex	Group	Protocol	Key Size		Classical	Quantum
ECDHE		TLSv1.1	256	yes	128	low
ECDHE		TLSv1.1	384	yes	192	low
ECDHE		TLSv1.1	256	yes	128	low
ECDHE		TLSv1.1	256	yes	128	low
RSA		TLSv1.2	4096	no	150	low
RSA		TLSv1.2	4096	no	150	low
RSA		TLSv1.2	4096	no	150	low
RSA		TLSv1.2	4096	no	150	low
RSA		TLSv1.2	4096	no	150	low
RSA		TLSv1.2	4096	no	150	low
RSA		TLSv1.2	4096	no	150	low
RSA		TLSv1.2	4096	no	150	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	3072	yes	132	low
DHE		TLSv1.2	4096	yes	150	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	3072	yes	132	low
DHE		TLSv1.2	4096	yes	150	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	3072	yes	132	low
DHE		TLSv1.2	4096	yes	150	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	3072	yes	132	low
DHE		TLSv1.2	4096	yes	150	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	3072	yes	132	low
DHE		TLSv1.2	4096	yes	150	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	3072	yes	132	low
DHE		TLSv1.2	4096	yes	150	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	3072	yes	132	low

Kex	Group	Protocol	Key Size		Classical	Quantum
DHE		TLSv1.2	4096	yes	150	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	3072	yes	132	low
DHE		TLSv1.2	4096	yes	150	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low

Kex	Group	Protocol	Key Size		Classical	Quantum
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (1)

None (1)

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

monografije.nitra.gov.r

Finding #	73885	**Severity**	Information Gathered - Level 1
Unique #	da292a86-0249-45e4-84af-2086decec9db		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The following is a list of detected SSL/TLS protocol properties.

Impact

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	monografije.nitra.gov.rs
IP	10.2.34.254
Port	443
Result	#table cols="2" NAME STATUS TLSv1 _ Extended_Master_Secret yes Encrypt_Then_MAC no Heartbeat no Truncated_HMAC no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no TLSv1.1 _ Extended_Master_Secret yes Encrypt_Then_MAC no Heartbeat no Truncated_HMAC no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no TLSv1.2 _ Extended_Master_Secret yes Encrypt_Then_MAC no Heartbeat no Truncated_HMAC no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no

Info List

Info #1

Props

Name	Value	Protocol
Extended Master Secret	yes	TLSv1
Encrypt Then MAC	no	TLSv1
Heartbeat	no	TLSv1
Truncated HMAC	no	TLSv1
Cipher priority controlled by	server	TLSv1
OCSP stapling	no	TLSv1
SCT extension	no	TLSv1
Extended Master Secret	yes	TLSv1.1
Encrypt Then MAC	no	TLSv1.1
Heartbeat	no	TLSv1.1
Truncated HMAC	no	TLSv1.1
Cipher priority controlled by	server	TLSv1.1
OCSP stapling	no	TLSv1.1
SCT extension	no	TLSv1.1
Extended Master Secret	yes	TLSv1.2
Encrypt Then MAC	no	TLSv1.2
Heartbeat	no	TLSv1.2
Truncated HMAC	no	TLSv1.2
Cipher priority controlled by	server	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2

42350 TLS Secure Renegotiation Extension Support Information (1)

None (1)

42350 TLS Secure Renegotiation Extension Support Information

monografije.nitra.gov.r

Finding #	73879	**Severity**	Information Gathered - Level 1
Unique #	a97522c8-9780-40aa-8551-dd4968368997		

Group	Scan Diagnostics		
CWE	-	Detection Date	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	monografije.nitra.gov.rs
IP	10.2.34.254
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

45038 Host Scan Time - Scanner (1)

None (1)

45038 Host Scan Time - Scanner

monografije.nitra.gov.r

Finding #	73868	Severity	Information Gathered - Level 1
Unique #	f9b5c846-d480-4c47-8a0b-56d935319342		
Group	Scan Diagnostics		
CWE	-	Detection Date	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

Impact
N/A

Solution
N/A

Results

Scan duration: 729 seconds

Start time: Fri, Jun 05 2026, 06:03:20 GMT

End time: Fri, Jun 05 2026, 06:15:29 GMT

6 DNS Host Name (1)

None (1)

6 DNS Host Name

monografije.nitra.gov.r

Finding #	73876	**Severity**	Information Gathered - Level 1
Unique #	9569a6b2-3c19-4c5e-8f75-7ac4d02bef61		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	10.2.34.254
Port	-
Result	#table IP_address Host_name 10.2.34.254 No_registered_hostname

86002 SSL Certificate - Information (1)

None (1)

86002 SSL Certificate - Information

monografije.nitra.gov.r

Finding #	73877	**Severity**	Information Gathered - Level 1

WAS Web Application Report

Unique #	bafa6c6c-9016-4233-8d0e-2906f3d3bd4e		
Group	Scan Diagnostics		
CWE	-	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	-		
WASC	-		

Details

Threat
SSL certificate information is provided in the Results section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	monografije.nitra.gov.rs
IP	10.2.34.254
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _78:e9:2d:47:e2:13:8c:7a:e0:a9:00:d0:bf:e0:58:48_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName GR _organizationName Hellenic_Academic_and_Research_Institutions_CA _commonName GEANT_TLS_RSA_1 (0)SUBJECT_NAME _ countryName RS _localityName \D0\91\D0\B5\D0\BE\D0\B3\D1\80\D0\B0\D0\B4 _organizationNam \D0\9C\D0\98\D0\9D\D0\98\D0\A1\D0\A2\D0\90\D0\A0\D0\A1\D0\A2\D0\92\D0\9E_\D0\9F\D0\A0\D0\9E\D0\A1\D0\92\D0\95\D0\A2\D0\95 _commonName *.nitra.gov.rs (0)Valid_From Dec_15_09:52:07_2025_GMT (0)Valid_Till Dec_15_09:52:07_2026_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (4096_bit) (0) _RSA_Public-Key:_(4096_bit) (0) _Modulus: (0) _00:af:83:37:4a:87:3e:42:fd:f7:7d:f5:df:07:82: (0) _b1:88:0f:46:8b:13:b8:b5:de:4c:a8:b7:38:18:fe: (0) _d3:c1:9f:b2:eb:4b:93:d7:e3:2a:80:dd:78:55:0c: (0) _e1:57:52:55:3d:9f:52:eb:bb:4c:d9:43:65:c9:87: (0) _a8:5a:44:ef:72:81:2a:6b:79:fe:a6:1f:6b:b5:12: (0) _6a:ec: 95:ec:e2:6c:44:54:74:da:54:0e:0c:dd:2a: (0) _93:92:27:8c:ad:67:5c:29:be:6e:46:6d:ab:ed:22: (0) _1c:d3:32:78:61:16:a2:bf:26:60:69:f0:2f:84:7c: (0) _98:d3:7e:a5:33:34:94:01:42:a2:e2:ca:19:df:7f: (0) _a1:33:a0:0b:c7:8f:e3:ee:30:d5:fb:69:20:b2:5a: (0) _24:85:42:0e:65:2e:2e:ad:9f:46:6e:68:f8:63:e7: (0) _21:b5:f6:8c:3c:a4:b2:a0:26:86:50:7e:50:96:63: (0) _c7:1d:68:72:4c:aa:95:0d:79:f4:d0:ab:4c:54:0f: (0) _70:57:bc:72:e1:b1:36:ef:ec:68:52:29:5d:42:91: (0) _75:69:00:64:a7:da:15:a4:18:c4:06:7f:04:ca:c8: (0) _56:50:26:b5:20:22:a8:9d:3f:6d:b2:cf:46:fc:30: (0) _51:b4:f9:e3:83:41:dd:c1:04:74:6e:97:ed:54:10: (0) _51:e1:33:38:4f:d6:0e:da:c8:3a:5c:01:b6:9f:48: (0) _57:69:0d:23:4f:1f:98:19:1f:57:3a:1a:49:07:94: (0) _0b:1c:93:3d:22:c5:4e:cf:3f:16:f4:b8:1e:48:d5: (0) _f0:f2:aa: 50:34:10:14:66:4e:2b:d3:1b:e5:30:49: (0) _b1:5e:e2:7e:fc:d4:82:c5:28:e5:06:7a:8e:19:5f: (0) _1c:d4:64:34:6c:57:61:fd:85:a4:39:cf:fc:55:4e: (0) _f2:d7:a4:59:93:b5:85:dd:b4:0d:2e:25:0b:13:55: (0) _dd:f5:51:04:3a:ee:68:8d:ae:64:f6:95:6c:37:fe: (0) _8b:51:af:50:27:cf:7d:85:98:c6:5f:7f:3d:79:60: (0) _a0:60:78:66:ad:78:8a:f4:42:c8:2c:d5:9f:08:47: (0) _0b:b2:2d:ee:d5:16:1b:a6:25:15:f7:79:25:cf:ba: (0) _26:f5:94:e4:3c:2f:9f:0f:cf:08:83:f8:9b:ec:8c: (0) _de:f6:ab:ea 10:45:af:b2:85:11:12:f7:9a:86:7e: (0) _64:61:75:77:34:95:b0:88:79:44:0b:37:65:2a:b0: (0) _fb:c2:82:86:87:95:37:fc:fc:31:26:7c:cc:91:9b: (0) _11:5a:5e:b0:a0:f1:a1: 74:a2:b9:1c:9a:48:e9: (0) _74:b9:59:b6:23:d0:2f:b8:b9:f3:c0:87:85:0e:aa: (0) _7c:e6:1f (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Basic_Constraints critical (0) _CA:FALSE (0)X509v3_Authority_Key_Identifier _keyid:86:01:72:3F:8C:A9:70:E2:31:06:53:16:CE:01:5F:5B:79:C8:3C:3E (0)Authority_Information_Access _CA_Issuers_-_URI:http://crt.harica.gr/HARICA-GEANT-TLS-R1.cer (0) _OCSP_-_URI:http://ocsp-tls.harica.gr (0)X509v3_Subject_Alternative_Name _DNS:*.nitra.gov.rs,_DNS:nitra.gov.rs (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.2 (0) _Policy:_0.4.0.2042.1.7 (_Policy:_1.3.6.1.4.1.26513.1.1.1.2 (0)X509v3_Extended_Key_Usage _TLS_Web_Client_Authentication,_TLS_Web_Server_Authentication (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl.harica.gr/HARICA-GEANT-TLS-R1.crl (0)X509v3_Subject_Key_Identifier _F7:C3:98:B0:F4:33:AE:1E:6F:BC:3D:BD:E9:6E:0C:6C:37:FB:C8:99 (0)X509v3_Key_Usage critical (0) _Digital_Signature,_Key_Encipherment (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_94:4E:43:87:FA:EC:C1:EF:81:F3:19:24:26:A8:18:65: (0) _01:C7:D3:5F:38:02:01:3F:72:67:7D:55:37:2E:19:D8 (0) _Timestamp_:_Dec_15_10:02:08.939_2025_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:21:00:AB:70:71:CD:16:7E:33:A7:A6:F1:AD: (0) _3F:53:21:02:43:EC:C1:A3:C4:8A:B1:E9:84:76:24:1C: (0) _F5:B5:36:43:F7:02:20:6E:2C: 49:2D:9A:ED:C0:25:74: (0) _C7:CB:A1:D7:A3:19:4F:68:6B:D8:F4:CF:BE:A7:15:3C: (0) _C8:9F:22:6D:18:F6:89 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_D7:6D:7D:10:D1:A7:F5:77:C2:C7:E9:5F:D7:00:BF:F9: (0) _82:C9:33:5A:65:E1:D0:B3:01:73:17:C0:C8:C5:69:77 (0) _Timestamp_:_Dec_15_10:02:08.948_2025_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:66:AD:20:40:11:E1:03:EE:6B: 59:8A:AA: (0) _4E:6F:2D:78:D8:15:D6:04:A7:F6:B2:58:AF:74:98:14: (0) _6B:69:B2:27:02:21:00:86:1A:BC:AE:3E:3B:5F:9B:30: (0) _42:D9:D3:50:F9:14:33:6C: 99:81:7C:05:2F:B7:E9:03: (0) _7D:FF:5C:9F:23:01:4D (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_D8:09:55:3B:94:4F: 7A:FF:C8:16:19:6F:94:4F:85:AB: (0) _B0:F8:FC:5E:87:55:26:0F:15:D1:2E:72:BB:45:4B:14 (0) _Timestamp_:_Dec_15_10:02:08.889_2025_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:45:02:20:59:DC:8D:9D:B6:C2:94:0E:88:6A:4F:F9: (0) _97:62:9C:92:D1:0D:FA: 0B:F2:5D:A3:07:DD:EF:95:16: (0) _8B:22:60:46:02:21:00:DB:3E:A6:69:35:A6:7C:DC:78: (0) _A8:29:F5:C6:E3:60:6C:C2:89:41:89:59:89:C8:8D:19: (0) _5B:56:8A: 65:FA:5B:C1 (0)Signature (384_octets) (0) 68:ef:db:f1:60:00:41:de:b3:72:d4:b8:58:a7:6e:01 (0) 85:0c:bd:b4:44:84:35:ed:da:1d:c6:64:da:cf:60:94 (0) 5f:dc:ab: 00:61:53:aa:80:c6:b0:9d:e3:95:30:ca:b6 (0) ae:8e:55:bb:77:aa:9c:6e:76:56:b3:6d:45:b1:1a:ab (0) db:02:9f:f8:e7:0f:c0:44:2b:15:e6:4e:15:cf:16:e7 (0) bd:76:35:ce:d 31:a9:d9:95:81:a9:c8:64:f8:79:28 (0) ab:86:6b:c1:60:21:a4:f1:38:b2:08:00:a8:a8:19:c3 (0) ec:ec:f2:e8:2b:bf:92:6d:3a:98:4b:54:60:10:c2:4b (0) 0c: 8e:ca:cd:d3:a1:b7:95:5c:4f:3e:33:fd:bc:c3:eb (0) 9f:92:d0:8b:50:3b:3d:c2:1d:00:34:5b:f6:a9:0a:50 (0) 04:5d:3d:19:18:87:55:25:5f:8e:dd:31:22:18:77:de (0) 8e: 96:06:9d:ad:92:72:1e:e5:d5:6c:ef:ad:31:ae:da (0) e7:33:88:47:03:42:d7:2a:00:c5:6b:0c:8c:b0:54:bc (0) 06:8c:6d:24:59:71:7d:ac:9f:9c:f0:64:11:c6:49:e5 (0) 1f:54:0

09:71:55:61:ac:59:ad:41:ee:cf:12:33:04 (0) a6:ec:c9:12:46:e7:8c:0f:e6:c9:70:49:90:b5:56:93 (0) 14:24:7b:f3:55:10:6a:15:52:25:93:d3:95:1d:87:61 (0) 65:d2:a1:91
24:ea:ab:13:7e:e3:a7:f2:59:07:7d (0) 08:7a:52:db:c1:64:4f:30:d6:83:18:d1:58:26:99:06 (0) 4c:23:80:74:84:79:7f:89:98:d5:f7:17:c1:1b:0f:ef (0) 34:d9:d7:36:b3:b3:5
82:d8:89:cd:72:bd:e6:6a (0) 52:cd:7d:13:1d:41:7a:8f:63:ae:d5:c4:2d:37:00:df (0) e2:3a:67:fc:43:ae:10:df:34:a6:94:93:d4:96:7d:8a (0) 2d:0a:05:25:e9:a4:fe:
31:39:97:ab:b4:62:09:1e:82 (1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number _14:d5:7b:f3:69:22:28:21:9a:55:67:fa:91:65:1b:22_ (1)Signature_Algorit
sha256WithRSAEncryption (1)ISSUER_NAME _ countryName GR _organizationName Hellenic_Academic_and_Research_Institutions_CA _commonName
HARICA_TLS_RSA_Root_CA_2021 (1)SUBJECT_NAME _ countryName GR _organizationName Hellenic_Academic_and_Research_Institutions_CA
_commonName GEANT_TLS_RSA_1 (1)Valid_From Jan_3_11:15:00_2025_GMT (1)Valid_Till Dec_31_11:14:59_2039_GMT (1)Public_Key_Algorithm
rsaEncryption (1)RSA_Public_Key (3072_bit) (1) _RSA_Public-Key:_(3072_bit) (1) _Modulus: (1) _00:a1:04:69:94:b3:13:3c:e7:00:f9:3c:20:46:b5: (1) _ec:
64:86:c8:9c:cf:4e:3e:1c:c1:16:3b:fe:f7:2a: (1) _d8:13:d3:e7:e2:11:1b:14:2d:68:27:60:2d:72:04: (1) _97:67:1d:3d:d2:24:8f:67:b2:6a:41:66:80:c8:c0: (1)
_b7:27:a3:bb:c5:7c:75:16:b2:40:20:ff:6d:68:c9: (1) _ee:d8:43:96:8c:20:2e:58:d0:69:78:ab:c6:76:1b: (1) _4f:c6:f3:44:70:21:09:9a:81:6a:46:20:8b:92:96: (1)
_c3:d7:40:34:bc:83:1c:6a:57:51:d6:36:e7:d6:9b: (1) _d2:55:84:68:51:39:52:ee:88:cd:04:8c:24:e0:32: (1) _e2:5f:d3:c3:29:bc:19:48:b2:d2:a3:03:10:11:52: (1)
_96:6d:f5:0b:d0:57:a5:d1:ca:28:09:61:bc:88:cc: (1) _88:aa:03:79:35:a5:e6:f6:5a:2c:1d:8c:31:11:98: (1) _d7:25:b6:7e:d3:e0:20:fd:3f:32:45:f5:b8:52:13: (1)
_96:f1:e6:98:c4:e7:83:1a:65:1f:59:f2:6c:42:09: (1) _16:2c:07:83:52:a2:2e:4d:53:a6:b7:19:81:e3:b6: (1) _83:11:39:2f:3d:f0:4c:55:ab:b1:49:40:ce:b8:79: (1) _c5:69:
71:69:23:36:2f:f8:06:97:ae:89:3e:7e: (1) _34:4c:45:73:36:e8:2e:75:ce:7e:3b:9c:8b:fe:db: (1) _b2:73:e2:d7:f6:99:37:f8:8a:35:b2:51:9e:78:05: (1) _a0:b6:8a:54:c9:a
09:2e:d7:a3:7e:1f:f8:12:13: (1) _6a:da:f2:41:91:44:bb:6a:03:28:4c:50:1a:5c:43: (1) _04:27:d8:30:b8:0b:b9:c5:ff:a2:7a:4b:cd:44:a0: (1) _79:02:13:34:bc:7a:8b:9b:
46:19:b5:18:1f:ef:43: (1) _cb:71:88:eb:a2:ff:e6:d3:e3:ab:39:4e:b3:27:64: (1) _8b:c6:58:18:4e:52:04:97:96:09:9d:88:ae:15:1e: (1) _d1:6c:d9:d9:be:99:86:4e:89:01
_Exponent:_65537_(0x10001) (1)X509v3_EXTENSIONS _ (1)X509v3_Basic_Constraints critical (1) _CA:TRUE,_pathlen:0 (1)X509v3_Authority_Key_Identifier
_keyid:0A:48:23:A6:60:A4:92:0A:33:EA:93:5B:C5:57:EA:25:4D:BD:12:EE (1)Authority_Information_Access _CA_Issuers_-_URI:http://crt.harica.gr/HARICA-TLS-
Root-2021-RSA.cer (1)X509v3_Certificate_Policies _Policy:_X509v3_Any_Policy (1)X509v3_Extended_Key_Usage
_TLS_Web_Client_Authentication,_TLS_Web_Server_Authentication (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl.harica.gr/HARICA-
Root-2021-RSA.crl (1)X509v3_Subject_Key_Identifier _86:01:72:3F:8C:A9:70:E2:31:06:53:16:CE:01:5F:5B:79:C8:3C:3B (1)X509v3_Key_Usage critical (1)
_Digital_Signature,_Certificate_Sign,_CRL_Sign (1)Signature (512_octets) (1) 19:2c:b2:34:33:62:b3:a8:e0:63:2c:29:e8:1a:0a:13 (1) f5:eb:
23:5e:e9:27:24:71:60:72:98:ce:39:e5:1d:ab (1) 31:eb:90:df:39:71:50:d3:84:b7:e2:94:7e:0b:9e:38 (1) 0d:ae:ae:9e:23:e9:39:4f:6e:cf:d7:c6:9c:2e:37:72 (1) 35:7f:4f:
4b:ba:4e:5b:f9:98:11:5c:ce:e8:6c:4e:99 (1) 2d:37:ab:55:05:8a:a1:34:a1:ca:5d:f8:47:65:e5:2b (1) ca:44:cb:bf:ba:ec:7b:78:95:c2:73:b7:e2:ba:2b:98 (1) 04:ba:
83:d2:19:00:cf:79:ff:9f:51:f9:97:ac:57:20 (1) 04:c7:0c:6e:d7:c3:6f:d7:6e:6c:52:8d:65:9c:68:e6 (1) 70:17:8a:a8:45:30:e2:32:07:26:a0:dc:7f:ad:39:3b (1) 87:f3:3b:
88:77:da:47:44:3b:14:a4:02:07:27:df:d6 (1) d9:60:5f:2d:c2:9a:bf:b2:0a:46:53:41:44:3f:ec:3c (1) 1c:bd:d3:72:7d:58:73:ca:c2:5f:24:41:20:c0:f9:a6 (1) bb:5c:
26:24:ed:b2:6d:13:27:fe:ec:63:3d:17:97:19 (1) ef:e6:32:92:75:ea:9e:ff:eb:b5:01:24:4c:a6:5d:42 (1) 8e:54:b3:5f:15:15:ef:6a:aa:3f:78:b5:76:cb:76:4e (1) cf:7a:
32:58:34:1e:0e:66:59:62:e3:82:dd:ee:bb:6a (1) 7c:59:54:c9:c8:7b:80:8c:45:3a:68:b2:c4:c4:10:62 (1) b6:26:52:2f:bb:e2:51:19:bd:fa:0d:86:ea:de:7f:40 (1)
ae:a6:e2:a9:cf:a3:b7:74:bb:fa:90:ef:53:d7:4b:8d (1) 74:30:68:05:04:e4:81:ed:d4:cc:76:9f:4c:87:b7:47 (1) 6a:37:ba:35:ca:50:63:f0:c9:cf:66:ef:f1:44:4f:22 (1) 8b:50:
12:53:fe:4e:01:53:9e:04:25:3c:42:d9:0a (1) 2a:33:3c:02:66:e9:2a:97:b7:a4:75:9c:ca:ad:d1:ec (1) 1d:cb:98:80:0b:90:c3:d3:c9:dc:83:7f:17:a7:eb:92 (1) 03:a9:11:1b
56:af:0d:c6:38:64:25:38:54:cf:8d:09 (1) a8:e9:4d:ea:ea:8a:a9:e0:c8:4a:3f:c8:a2:e7:18:c2 (1) ca:96:db:80:25:3b:b6:73:36:6a:21:42:63:22:f1:ea (1) 76:dc:7e:
21:05:28:74:18:14:de:d9:7b:e4:bb:36:8d (1) 7f:dd:ac:c8:af:25:d8:7c:ce:fb:5d:c6:2c:28:f3:60 (1) b4:cf:bd:74:ce:f5:4a:4a:f0:31:b2:7c:66:4e:b9:a9 (1) ae:c1:b0:27:6c
44:dd:17:e3:57:d2:1a:51:01:89 (2)CERTIFICATE_2 _ (2)Version 3_(0x2) (2)Serial_Number _39:ca:93:1c:ef:43:f3:c6:8e:93:c7:f4:64:89:38:7e_
(2)Signature_Algorithm sha256WithRSAEncryption (2)ISSUER_NAME _ countryName GR _organizationName Hellenic_Academic_and_Research_Institutions_
_commonName HARICA_TLS_RSA_Root_CA_2021 (2)SUBJECT_NAME _ countryName GR _organizationName
Hellenic_Academic_and_Research_Institutions_CA _commonName HARICA_TLS_RSA_Root_CA_2021 (2)Valid_From Feb_19_10:55:38_2021_GMT (2)Valid_
Feb_13_10:55:37_2045_GMT (2)Public_Key_Algorithm rsaEncryption (2)RSA_Public_Key (4096_bit) (2) _RSA_Public-Key:_(4096_bit) (2) _Modulus: (2)
_00:8b:c2:e7:af:65:9b:05:67:96:c9:0d:24:b9:d0: (2) _0e:64:fc:ce:e2:24:18:2c:84:7f:77:51:cb:04:11: (2) _36:b8:5e:ed:69:71:a7:9e:e4:25:09:97:67:c1:47: (2) _c2:cf
91:16:36:62:3d:38:04:e1:51:82:ff:ac:d2: (2) _b4:69:dd:2e:ec:11:a3:45:ee:6b:6b:3b:4c:bf:8c: (2) _8d:a4:1e:9d:11:b9:e9:38:f9:7a:0e:0c:98:e2:23: (2) _1d:d1:4e:
63:d4:e7:b8:41:44:fb:6b:af:6b:da:1f: (2) _d3:c5:91:88:5b:a4:89:92:d1:81:e6:8c:39:58:a0: (2) _d6:69:43:a9:ad:98:52:58:6e:db:0a:fb:6b:cf:68: (2) _fa:e3:a4:5e:3a:
45:73:98:07:ea:5f:02:72:de:0c: (2) _a5:b3:9f:ae:a9:1d:b7:1d:b3:fc:8a:59:e7:6e:72: (2) _65:ad:f5:30:94:23:07:f3:82:16:4b:35:98:9c:53: (2) _bb:2f:ca:e4:5a:d9:c7:8
1d:fc:98:99:fb:2c:a4: (2) _82:6b:f0:2a:1f:8e:0b:5f:71:5c:5c:ae:42:7b:29: (2) _89:81:cb:03:a3:99:ca:88:9e:0b:40:09:41:33:db: (2) _e6:58:7a:fd:ae:99:70:c0:5a:
0f:d6:13:86:71:2f: (2) _76:69:fc:90:dd:db:2d:6e:d1:f2:9b:f5:1a:6b:9e: (2) _6f:15:8c:7a:f0:4b:28:a0:22:38:80:24:6c:36:a4: (2) _3b:f2:30:91:f3:78:13:cf:c1:3f:35:ab:f1
11: (2) _23:b5:43:22:9e:01:92:b7:18:02:e5:11:d1:82:db: (2) _15:00:cc:61:37:c1:2a:7c:9a:e1:d0:ba:b3:50:46: (2) _ee:82:ac:9d:31:f8:fb:23:e2:03:00:48:70:a3:09: (2
_26:79:15:53:60:f3:38:5c:ad:38:ea:81:00:63:14: (2) _b9:33:5e:dd:0b:db:a0:45:07:1a:33:09:f8:4d:b4: (2) _a7:02:a6:69:f4:c2:59:05:88:65:85:56:ae:4b:cb: (2) _e0:d
7d:2d:1a:c8:e9:fb:1f:a3:61:4a:d6:2a: (2) _13:ad:77:4c:1a:18:9b:91:0f:58:d8:06:54:c5:97: (2) _f8:aa:3f:20:8a:a6:85:a6:77:f6:a6:fc:1c:e2:ee: (2) _6e:94:33:2a:
83:50:84:0a:e5:4f:86:f8:50:45:78: (2) _00:81:eb:5b:68:e3:26:8d:cc:7b:5c:51:f4:14:2c: (2) _40:be:1a:60:1d:7a:72:61:1d:1f:63:2d:88:aa:ce: (2) _a2:45:90:08:fc:
6b:be:b3:50:2a:5a:fd:a8:48:18: (2) _46:d6:90:40:92:90:0a:84:5e:68:31:f8:eb:ed:0d: (2) _d3:1d:c6:7d:99:18:55:56:27:65:2e:8d:45:c5:24: (2) _ec:ce:e3 (2)
_Exponent:_65537_(0x10001) (2)X509v3_EXTENSIONS _ (2)X509v3_Basic_Constraints critical (2) _CA:TRUE (2)X509v3_Subject_Key_Identifier _0A:
48:23:A6:60:A4:92:0A:33:EA:93:5B:C5:57:EA:25:4D:BD:12:EE (2)X509v3_Key_Usage critical (2) _Digital_Signature,_Certificate_Sign,_CRL_Sign (2)Signature
(512_octets) (2) 3e:90:48:aa:6e:62:15:25:66:7b:0c:d5:8c:8b:89:9d (2) d7:ed:4e:07:ef:9c:d0:14:5f:5e:50:bd:68:96:90:a4 (2) 14:11:aa:68:6d:09:35:39:40:09:da:f4:0
34:a5 (2) 7b:59:84:49:29:97:74:c8:07:1e:47:6d:f2:ce:1c:50 (2) 26:e3:9e:3d:40:53:3f:f7:7f:96:76:10:c5:46:a5:d0 (2) 20:4b:50:f4:35:3b:18:f4:55:6a:41:1b:47:06:68:3
(2) bb:09:08:62:d9:5f:55:42:aa:ac:53:85:ac:95:56:36 (2) 56:ab:e4:05:8c:c5:a8:da:1f:a3:69:bd:53:0f:c4:ff (2) dc:ca:e3:7e:f2:4c:88:86:47:46:1a:f3:00:f5:80:91 (2) a2
43:42:94:9b:20:f0:d1:cd:b2:eb:2c:53:c2:53 (2) 78:4a:4f:04:94:41:9a:8f:27:32:c1:e5:49:19:bf:f1 (2) f2:c2:8b:a8:0a:39:31:28:b4:7d:62:36:2c:4d:ec:1f (2) 33:b6:7e:7
7e:50:f0:9f:0e:d7:11:8f:cf:18:c5 (2) e3:27:fe:26:ef:05:9d:cf:cf:37:c5:d0:7b:da:3b:b0 (2) 16:84:0c:3a:93:d6:be:17:db:0f:3e:0e:19:78:09:c7 (2)
a9:02:72:22:4b:f7:37:76:ba:75:c4:85:03:5a:63:d5 (2) b1:75:05:c2:b9:bd:94:ad:8c:15:99:a7:93:7d:f6:c5 (2) f3:aa:74:cf:04:85:94:98:00:f4:e2:f9:ca:24:65:bf (2)
e0:62:af:c8:c5:fa:b2:c9:9e:56:48:da:79:fd:96:76 (2) 15:be:a3:8e:56:c4:b3:34:fc:be:47:f4:c1:b4:a8:fc (2) d5:30:88:68:ee:cb:ae:c9:63:c4:76:be:ac:38:18:e1 (2) 5e:
5c:cf:ae:3a:22:51:eb:d1:8b:b3:f3:2b:33:07:54 (2) 87:fa:b4:b2:13:7b:ba:53:04:62:01:9d:f1:c0:4f:ee (2) e1:3a:d4:8b:20:10:fa:02:57:e6:ef:c1:0b:b7:90:46 (2) 9c:
19:29:8c:dc:6f:a0:4a:69:69:94:b7:24:65:a0:ff (2) ac:3f:ce:01:fb:21:2e:fd:68:f8:9b:f2:a5:cf:31:38 (2) 5c:15:aa:e6:97:00:c1:df:5a:a5:a7:39:aa:e9:84:7f (2) 3c:
51:a8:3a:d9:94:5b:8c:bf:4f:08:71:e5:db:a8:5c (2) d4:d2:a6:fe:00:a3:c6:16:c7:0f:e8:80:ce:1c:28:64 (2) 74:19:08:d3:42:e3:ce:00:5d:7f:b1:dc:13:b0:e1:05 (2)
cb:d1:20:aa:86:74:9e:39:e7:91:fd:ff:5b:d6:f7:ad (2) a6:2f:03:0b:6d:e3:57:54:eb:76:53:18:8d:11:98:ba

Info List

Info #1

Certificate Fingerprint:33FF9BC27A3440E8FA7E5336F4D802F4E95D7514370672C6C95B1873D518D3C5

Info #2

Certificate Fingerprint:33FF9BC27A3440E8FA7E5336F4D802F4E95D7514370672C6C95B1873D518D3C5

Info #3

Certificate Fingerprint:33FF9BC27A3440E8FA7E5336F4D802F4E95D7514370672C6C95B1873D518D3C5

Security Weaknesses (7)

150202 Missing header: X-Content-Type-Options (1)

None (1)

150202 Missing header: X-Content-Type-Options — *monografije.nitra.gov.r*

Finding #	73871	**Severity**	Information Gathered - Level 2
Unique #	05605334-9b99-4352-87f1-9cb7e89b5c90		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Content-Type-Options response header is not present. WAS reports missing X-Content-Type-Options header on each crawled link for both static and dynamic responses. The scanner performs the check not only on 200 responses but 4xx and 5xx responses as well. It's also possible the QID will be reported on directory-level links.

Impact

All web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. If X-Content-Type-Options header is not present, browsers can potentially be tricked into treating non-HTML response as HTML. An attacker can then potentially leverage the functionality to perform a cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack.

Solution

It is recommended to disable browser content sniffing by adding the X-Content-Type-Options header to the HTTP response with a value of 'nosniff'. Also, ensure that the 'Content-Type' header is set correctly on responses.

Results

X-Content-Type-Options: Header missing
Response headers on link: GET https://monografije.nitra.gov.rs/. response code: 200
Date: Fri, 05 Jun 2026 06:08:07 GMT
Last-Modified: Fri, 07 Apr 2023 11:06:55 GMT
ETag: "0-5f8bd05e8ab18"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; domain=.monografije.nitra.gov.rs; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://monografije.nitra.gov.rs/. response code: 200
GET https://monografije.nitra.gov.rs/ response code: 200

150206 Content-Security-Policy Not Implemented (1)

None (1)

150206 Content-Security-Policy Not Implemented — *monografije.nitra.gov.r*

WAS Web Application Report

Finding #	73875	**Severity**	Information Gathered - Level 2
Unique #	51e71492-f562-40b4-b903-adb2000b6404		
Group	Security Weaknesses		
CWE	CWE-829, CWE-16, CWE-1032	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

Results

Content-Security-Policy: Header missing
Response headers on link: GET https://monografije.nitra.gov.rs/. response code: 200
Date: Fri, 05 Jun 2026 06:08:07 GMT
Last-Modified: Fri, 07 Apr 2023 11:06:55 GMT
ETag: "0-5f8bd05e8ab18"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; domain=.monografije.nitra.gov.rs; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://monografije.nitra.gov.rs/. response code: 200
GET https://monografije.nitra.gov.rs/ response code: 200

150208 Missing header: Referrer-Policy (1)

WAS Web Application Report

None (1)

150208 Missing header: Referrer-Policy

monografije.nitra.gov.r

Finding #	73861	**Severity**	Information Gathered - Level 2
Unique #	03d61c08-350d-485d-b437-e5e76effead8		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Referrer Policy header is used to control the flow of information from the source to the destination when a link is clicked. During the scan checks are done for the presence of the Referrer Policy on all static and dynamic pages. One of the following values for Referrer Policy in the response headers was found to be missing:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found, the response body is checked for a meta tag containing the tag name as "referrer" and one of the above Referrer Policy.
Missing referrer header is reported for links with the following response codes - 2XX, 4xx, and 5xx. Links that report a response code of 3xx will not be tested for presence of this header.

Impact

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

Solution

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Results

Referrer-Policy: Header missing
Response headers on link: GET https://monografije.nitra.gov.rs/. response code: 200
Date: Fri, 05 Jun 2026 06:08:07 GMT
Last-Modified: Fri, 07 Apr 2023 11:06:55 GMT
ETag: "0-5f8bd05e8ab18"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; domain=.monografije.nitra.gov.rs; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://monografije.nitra.gov.rs/. response code: 200
GET https://monografije.nitra.gov.rs/ response code: 200

150248 Missing header: Permissions-Policy (1)

None (1)

150248 Missing header: Permissions-Policy — *monografije.nitra.gov.r*

Finding #	73866	**Severity**	Information Gathered - Level 2
Unique #	8e242914-4d47-4e81-bbc1-6c0e3b36d3e2		
Group	Security Weaknesses		
CWE	CWE-284	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	A6 Security Misconfiguration		
WASC	-		

Details

Threat
The Permissions-Policy response header is not present.

Impact
Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

Solution
It is recommended to define policy for policy controlled features to make application more secure.

References:
Permissions-Policy W3C Working Draft
Policy Controlled Features

Results

Permissions-Policy: Header missing
Response headers on link: GET https://monografije.nitra.gov.rs/. response code: 200
Date: Fri, 05 Jun 2026 06:08:07 GMT
Last-Modified: Fri, 07 Apr 2023 11:06:55 GMT
ETag: "0-5f8bd05e8ab18"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; domain=.monografije.nitra.gov.rs; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://monografije.nitra.gov.rs/. response code: 200
GET https://monografije.nitra.gov.rs/ response code: 200

WAS Web Application Report

150823 HTTP TRACE Method Detected (1)

None (1)

150823 HTTP TRACE Method Detected

monografije.nitra.gov.r

Finding #	74155	**Severity**	Information Gathered - Level 2
Unique #	8589dec8-7870-46ff-807e-c631409af1b8		
Group	Security Weaknesses		
CWE	CWE-749	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	A6 Security Misconfiguration		
WASC	WASC-14 SERVER MISCONFIGURATION		

Details

Threat

HTTP defines methods (sometimes referred to as verbs) to indicate the desired action to be performed on the identified resource. TRACE and TRACK methods are defined by Apache and allow a user to echo the content of a request.
Diagnosis: Scan makes a request with TRACE method and looks for 200 response.

Impact

When TRACE or TRACK methods are available on the web server, attackers may perform an attack called "Cross site tracing". Due to the TRACK/TRACE methods, an attacker can echo sensitive headers from the web server, opening a way to steal sensitive information like cookies or authentication data.

Solution

Disable if TRACE method is not required.

Results

Request: https://monografije.nitra.gov.rs/
Comment: TRACE method is enabled (Unauth 200).

150142 Virtual Host Discovered (1)

None (1)

150142 Virtual Host Discovered

monografije.nitra.gov.r

Finding #	73874	**Severity**	Information Gathered - Level 1
Unique #	0933eff0-b03e-439a-b599-76ae157cef68		
Group	Security Weaknesses		
CWE	CWE-200	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	A6 Security Misconfiguration		
WASC	-		

Details

Threat

Web server is responding differently when the HOST header is manipulated and various common virtual hosts are tested. This could indicate the presence of Virtual Host. Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The extra virtual hosts discovered by the Web application scanner during HOST header manipulation are provided in the Results section.

Impact

The Web application should apply consistent security measures. If the Web application fails to apply security controls to other domains hosted on the same server, then it may be exposed to vulnerabilities like cross-site scripting, SQL injection, or authorization-based attacks.

Solution

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

Results

Virtual host discovered:

Detected based on: Unique redirect URI
Virtual Host: www.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://www.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: stage.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://stage.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: m.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://m.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: test.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://test.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: secure.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://secure.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: mail.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://mail.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: demo.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://demo.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: dev.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://dev.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: portal.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://portal.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: webmail.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://webmail.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: staging.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://staging.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: app.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://app.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: shop.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://shop.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: qa.monografije.nitra.gov.rs

URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://qa.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: apps.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://apps.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: admin.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://admin.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: login.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://login.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: online.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://online.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: mobile.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://mobile.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: store.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://store.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: blog.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://blog.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: beta.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://beta.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: api.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://api.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: extranet.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://extranet.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: web.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://web.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: intranet.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://intranet.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: services.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://services.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: support.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://support.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: connect.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://connect.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: email.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://email.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: remote.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://remote.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: images.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://images.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: orders.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://orders.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: merchant.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://merchant.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: retail.monografije.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://retail.monografije.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: www.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://www.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: stage.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://stage.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: m.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://m.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: test.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://test.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: secure.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://secure.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: mail.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://mail.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: demo.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://demo.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: dev.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://dev.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: portal.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://portal.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: webmail.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://webmail.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: staging.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://staging.nitra.gov.rs/

Detected based on: Unique redirect URI

Virtual Host: app.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://app.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: shop.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://shop.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: qa.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://qa.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: apps.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://apps.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: admin.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://admin.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: login.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://login.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: online.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://online.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: mobile.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://mobile.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: store.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://store.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: blog.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://blog.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: beta.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://beta.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: api.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://api.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: extranet.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://extranet.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: web.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://web.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: intranet.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://intranet.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: services.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://services.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: support.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/

Redirect URI(302): https://support.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: connect.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://connect.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: email.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://email.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: remote.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://remote.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: images.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://images.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: orders.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://orders.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: merchant.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://merchant.nitra.gov.rs/

Detected based on: Unique redirect URI
Virtual Host: retail.nitra.gov.rs
URI: http://monografije.nitra.gov.rs/
Redirect URI(302): https://retail.nitra.gov.rs/

150277 Cookie without SameSite attribute (1)

None (1)

150277 Cookie without SameSite attribute

monografije.nitra.gov.r

Finding #	73865	**Severity**	Information Gathered - Level 1
Unique #	e4fe1a53-9a50-419f-a41b-bb5ec14839bc		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	**Detection Date**	05 Jun 2026 08:03 GMT+0200
OWASP	A6 Security Misconfiguration		
WASC	-		

Details

Threat
The cookies listed in the Results section are missing the SameSite attribute.

Impact
The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

Solution
Consider adding the SameSite attribute to the cookie(s) listed.

More information:
DZone article
OWASP CSRF Prevention Cheat Sheet

Results

Total cookies: 1
TS011dbc9d=01875fe39c0f1e1fc228b5d780d0dadb46e94e6050d5f281e64356aed3b4db1e982318f99d85327fe38690ff048895088a44aab197; path=/; domain=.monografije.nitra.gov.rs | First set at URL: https://monografije.nitra.gov.rs/

WAS Web Application Report

Appendix

Web Application Details
monografije.nitra.gov.rs

Name	monografije.nitra.gov.rs
ID	325542
URL	http://monografije.nitra.gov.rs
Owner	Veljko Vesic (kance_vv)
Scope	Limit to URL hostname
Tags	-
Custom Attributes	-

Severity Levels
Confirmed Vulnerabilities

Vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

Minimal	**Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.**
Medium	**Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.**
Serious	**Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.**
Critical	**Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.**
Urgent	**Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.**

Potential Vulnerabilities

Potential Vulnerabilities indicate that the scanner observed a weakness or error that is commonly used to attack a web application, and the scanner was unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following-up with manual analysis. For example, the exploitability of a QID may be influenced by characteristics that the scanner cannot confirm, such as the web application's network architecture, or the test to confirm exploitability requires more intrusive testing than the scanner is designed to conduct.

Minimal	**Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.**
Medium	**Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.**
Serious	

	Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.
Critical	Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.
Urgent	Presence of this vulnerability might enable intruders to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. For example in this scenario, the web application users can potentially be targeted if the application is exploited.

Sensitive Content

Sensitive content may be detected based on known patterns (credit card numbers, social security numbers) or custom patterns (strings, regular expressions), depending on the option profile used. Intruders may gain access to sensitive content that could result in misuse or other exploits.

Minimal	Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.
Medium	Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.
Serious	Sensitive content was found in the web server response - a valid social security number or credit card information. This infomation disclosure could result in a confidentiality breach, and it gives intruders access to valid sensitive content that could be misused.

Information Gathered

Information Gathered issues (QIDs) include visible information about the web application's platform, code, or architecture. It may also include information about users of the web application.

Minimal	Intruders may be able to retrieve sensitive information related to the web application platform.
Medium	Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.
Serious	Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.