

ZAP by Checkmarx

Scanning Report

Generated with  ZAP on Mon 14 Apr 2025, at 16:22:15

ZAP Version: 2.16.1

ZAP by [Checkmarx](#)

Contents

- [About this report](#)
 - [Report parameters](#)
- [Summaries](#)
 - [Alert counts by risk and confidence](#)
 - [Alert counts by site and risk](#)
 - [Alert counts by alert type](#)
- [Alerts](#)
 - [Risk=High, Confidence=High \(1\)](#)
 - [Risk=High, Confidence=Medium \(5\)](#)
 - [Risk=Medium, Confidence=High \(1\)](#)
 - [Risk=Medium, Confidence=Medium \(4\)](#)
 - [Risk=Medium, Confidence=Low \(1\)](#)
 - [Risk=Low, Confidence=High \(3\)](#)
 - [Risk=Low, Confidence=Medium \(5\)](#)
 - [Risk=Low, Confidence=Low \(1\)](#)

- [Risk=Informational, Confidence=High \(2\)](#)
- [Risk=Informational, Confidence=Medium \(3\)](#)
- [Risk=Informational, Confidence=Low \(4\)](#)
- [Appendix](#)
 - [Alert types](#)

About this report

Report parameters

Contexts

The following contexts were selected to be included:

- PLIS

Sites

The following sites were included:

- <https://api.plis.sk>
- <https://auth.plis.sk>
- <https://www.plis.sk>

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: [High](#), [Medium](#), [Low](#), [Informational](#)

Excluded: None

Confidence levels

Included: [User Confirmed](#), [High](#), [Medium](#), [Low](#), [False Positive](#)

Excluded: None

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence					Total
		User Confirmed	High	Medium	Low	False Positive	
Risk	High	0 (0.0%)	1 (3.3%)	5 (16.7%)	0 (0.0%)	0 (0.0%)	6 (20.0%)
	Medium	0 (0.0%)	1 (3.3%)	4 (13.3%)	1 (3.3%)	0 (0.0%)	6 (20.0%)
	Low	0 (0.0%)	3 (10.0%)	5 (16.7%)	1 (3.3%)	0 (0.0%)	9 (30.0%)
	Informational	0 (0.0%)	2 (6.7%)	3 (10.0%)	4 (13.3%)	0 (0.0%)	9 (30.0%)
	Total	0 (0.0%)	7 (23.3%)	17 (56.7%)	6 (20.0%)	0 (0.0%)	30 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

Risk			
High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)

		Risk				Informational
		High (= High)	Medium (>= Medium)	Low (>= Low)	Low (>= Low)	
Site	https://api.plis.sk	0 (0)	0 (0)	4 (4)	1 (5)	
	https://auth.plis.sk	0 (0)	0 (0)	0 (0)	1 (1)	
	https://www.plis.sk	6 (6)	6 (12)	5 (17)	7 (24)	

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
PII Disclosure	High	2 (6.7%)
SQL Injection	High	1 (3.3%)
SQL Injection - MsSQL	High	4 (13.3%)
SQL Injection - Oracle - Time Based	High	78 (260.0%)
SQL Injection - SQLite	High	30 (100.0%)
Vulnerable JS Library	High	2 (6.7%)
Total		30

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	498 (1,660.0%)
Content Security Policy (CSP) Header Not Set	Medium	417 (1,390.0%)
Multiple X-Frame-Options Header Entries	Medium	412 (1,373.3%)
Potential IP Addresses Found in the Viewstate	Medium	11 (36.7%)
Secure Pages Include Mixed Content (Including Scripts)	Medium	2 (6.7%)
Vulnerable JS Library	Medium	8 (26.7%)
Cookie Without Secure Flag	Low	16 (53.3%)
Cookie without SameSite Attribute	Low	14 (46.7%)
Cross-Domain JavaScript Source File Inclusion	Low	498 (1,660.0%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	863 (2,876.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	897 (2,990.0%)
Strict-Transport-Security Header Not Set	Low	37 (123.3%)
Timestamp Disclosure - Unix	Low	2 (6.7%)
X-AspNet-Version Response Header	Low	575 (1,916.7%)
X-Content-Type-Options Header Missing	Low	851 (2,836.7%)
Total		30

Alert type	Risk	Count
Authentication Request Identified	Informational	1 (3.3%)
Charset Mismatch (Header Versus Meta Charset)	Informational	4 (13.3%)
GET for POST	Informational	2 (6.7%)
Information Disclosure - Suspicious Comments	Informational	167 (556.7%)
Modern Web Application	Informational	97 (323.3%)
Re-examine Cache-control Directives	Informational	235 (783.3%)
Session Management Response Identified	Informational	20 (66.7%)
User Agent Fuzzer	Informational	1382 (4,606.7%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	851 (2,836.7%)
Total		30

Alerts

Risk=High, Confidence=High (1)

<https://www.plis.sk> (1)

[PII Disclosure](#) (1)

▼ GET https://www.plis.sk/volne/hd/v_hd_rodokmen/v_hd_rodokmen.aspx?hd=SK000813847865

Alert tags

- [OWASP_2017_A03](#)
- [CWE-359](#)

	<ul style="list-style-type: none">▪ OWASP_2021_A04
Alert description	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
Other info	Credit Card Type detected: Maestro Bank Identification Number: 500948 Brand: MAESTRO Category: Issuer:
Request	<p>▼ Request line and header section (300 bytes)</p> <pre>GET https://www.plis.sk/volne/hd/v_hd_rodokmen/v_hd_rodokmen.aspx?hd=SK000813847865 HTTP/1.1 host: www.plis.sk user-agent: pragma: no-cache cache-control: no-cache referer: https://www.plis.sk/volne/hd/hd_p_DetailByk/z_hd_p_ZoznamByk.aspx Cookie: ASP.NET_SessionId=fxz2wlx0wzki4botxzazxsgl</pre> <p>▼ Request body (0 bytes)</p>
Response	<p>▼ Status line and header section (405 bytes)</p> <pre>HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 14 Apr 2025 12:50:59 GMT Content-Type: text/html; charset=windows-1250 Content-Length: 45171 Connection: keep-alive Vary: Accept-Encoding Cache-Control: private X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET</pre>

	X-FRAME-OPTIONS: SAMEORIGIN Strict-Transport-Security: max-age=63072000; includeSubdomains; preload X-Frame-Options: DENY
	► Response body (45171 bytes)
Evidence	500948700272
Solution	Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

Risk=High, Confidence=Medium (5)

https://www.plis.sk (5)	
SQL Injection (1)	
▼ POST https://www.plis.sk/volne/uni/Rozdelovnik/Rozdelovnik.aspx?typ=C	
Alert tags	<ul style="list-style-type: none">▪ POLICY_SEQUENCE =▪ OWASP_2021_A03▪ CWE-89▪ WSTG-v42-INPV-05▪ POLICY_API =▪ POLICY_DEV_FULL =▪ POLICY_QA_STD =▪ POLICY_QA_FULL =▪ OWASP_2017_A01▪ POLICY_DEV_CICD =▪ POLICY_DEV_STD =
Alert description	SQL injection may be possible.
Other info	<p>The page results were successfully manipulated using the boolean conditions [EFEC4011 AND 1=1 --] and [EFEC4011 AND 1=2 --]</p> <p>The parameter value being modified was NOT stripped from the HTML output for the purposes of</p>

the comparison.

Data was returned for the original parameter.

The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter.

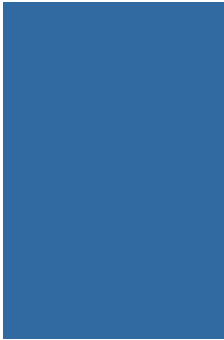
Request

▼ Request line and header section (356 bytes)

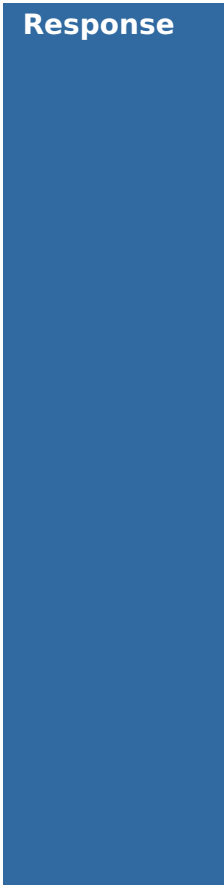
```
POST https://www.plis.sk/volne/uni/
Rozdelovnik/Rozdelovnik.aspx?typ=C
HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
content-type: application/x-www-form-
urlencoded
referer: https://www.plis.sk/volne/uni/
Rozdelovnik/Rozdelovnik.aspx?typ=C
content-length: 1085
Cookie:
ASP.NET_SessionId=fxz2wLx0wzki4botxzazxsgl
```

▼ Request body (1085 bytes)

```
__VIEWSTATE=%2FwEPDwUJODI10TEwMjM2D2QWAmYP
ZBYCAgMPZBYCAgEPZBYKZg8PFgIeBFRleHQFK1Z5aM
SC4oCew4TEvmFkYW5pZSB6dmllcmHDhMSFw4TigJ5h
IHYgUExJU2VkZAIbDw8WAh8ABQ1Wb8S%2Bbs0hIHrD
s25hZGQCBA8PFgIeB1Zpc2libGVoZGQCBQ8PFgIfAW
hkZAIJD2QWBAIGDw8WAh4LUG9zdEJhY2tVcmwFJGh0
dHBz0i8vd3d3LnBsaXMuc2svdm9sbmUvaGQvaGQuYX
NweGRkAgwPDxYCHwAFAUNKZBgBBR5fX0NvbRyb2xz
UmVxdWlyZVBvc3RCYWNRs2V5X18WAgUYY3RSMdAkTG
9naW5TdGF0dXMxJGN0bDAXBRhjdGwwMCRMb2dpblN0
YXR1czEkY3RSMd0JDPzsmP6Cq6rcbl9W0wLCZEmQhv
3v4EIljv8jKfcrfQ%3D%3D&__VIEWSTATEGENERATO
R=EFEC4011+AND+1%3D1+- -
+&__PREVIOUSPAGE=h3pBkKfLX8EG4xpgniCA-3FB3
CNEjIvnpheB9AGjRxyA8-
w0d0YeYsycPbS0nGugp15bvIQcGq93KyXua4pfmL2G
wwQDpu91yaDk-nl0ty3-
Ds_WR41KSWgwXQfQolPJ0&__EVENTVALIDATION=%2
FwEdAAi6M8S7NhDIfqmZHvBbyJZZFcm05kLBLcy80X
yCdqLipbgdV0yPamfwqon%2BU%2FkXWwTKGUcM3blp
```



wEw1ynmnEpiuDAPwfJ9mwk%2F7k4vn0lyfw9e5UqaS
KHmsbv3B%2F9k8v1CxXw0tg0Rg73I9WU%2B9fN%2BM
57W095nKSImdyGw0l0zc00pdb0kxdNJ8iSKuSwvT86
M0YEoN5HNqSUYH0LJIxW2n&ctl00%24ButtonPatch
=&ctl00%24ContentPlaceholder1%24HiddenFiel
d_TitulokHlavicka=Vyh%C4%82%E2%80%9E%C3%84
%C4%BEadanie+zviera%C3%84%C4%85%C3%84%E2%8
0%9Ea+v+PLISe



Response

▼ Status line and header section (405 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 13:36:25 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 21613
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

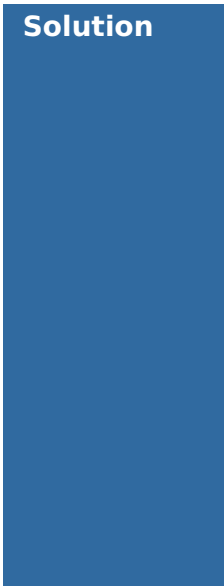
► Response body (21613 bytes)

Parameter

__VIEWSTATEGENERATOR

Attack

EFEC4011 AND 1=1 --



Solution

Do not trust client side input, even if there is client side validation in place.

In general, type check all data on the server side.

If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.

If database Stored Procedures can be used, use them.

Do **not** concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!

Do not create dynamic SQL queries using simple string concatenation.

Escape all data received from the client.

Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.

Apply the principle of least privilege by using the least privileged database user possible.

In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.

Grant the minimum database access that is necessary for the application.

SQL Injection - MsSQL (1)

▼ POST https://www.plis.sk/volne/hd/hd_p_DetailByk/z_hd_p_Detailbyk.aspx?zviera=SK000813837952

Alert tags

- POLICY_SEQUENCE =
- [OWASP_2021_A03](#)
- [CWE-89](#)
- [WSTG-v42-INPV-05](#)
- POLICY_DEV_FULL =
- POLICY_QA_STD =
- POLICY_QA_FULL =
- [OWASP_2017_A01](#)

Alert description

SQL injection may be possible.

Other info

The query time is controllable using parameter value [SK000813837952' WAITFOR DELAY '0:0:15' --], which caused the request to take [15,021] milliseconds, when the original

unmodified query with value [SK000813837952]
took [0] milliseconds.

Request

▼ Request line and header section (440 bytes)

```
POST https://www.plis.sk/volne/hd/
hd_p_DetailByk/z_hd_p_Detailbyk.aspx?
zviera=SK000813837952%27+WAITFOR+DELAY+
%270%3A0%3A15%27+- -+ HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
content-type: application/x-www-form-
urlencoded
referer: https://www.plis.sk/volne/hd/
hd_p_DetailByk/z_hd_p_Detailbyk.aspx?
zviera=SK000813837952
content-length: 7384
Cookie:
ASP.NET_SessionId=fxz2wlx0wzki4botxzazxsg
l
```

► Request body (7384 bytes)

Response

▼ Status line and header section (469 bytes)

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 14:36:31 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 191
Connection: keep-alive
Cache-Control: private
Location: /chybova.aspx?aspxerrorpath=/
volne/hd/hd_p_DetailByk/
z_hd_p_Detailbyk.aspx
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY
```

▼ Response body (191 bytes)

```
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/chybova.aspx?aspxerrorpath=/volne/hd/hd_p_DetailByk/z_hd_p_Detailbyk.aspx">here</a>.</h2>
</body></html>
```

Parameter

zviera

Attack

```
SK000813837952' WAITFOR DELAY '0:0:15'
--
```

Solution

Do not trust client side input, even if there is client side validation in place.

In general, type check all data on the server side.

If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.

If database Stored Procedures can be used, use them.

Do **not** concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!

Do not create dynamic SQL queries using simple string concatenation.

Escape all data received from the client.

Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.

Apply the principle of least privilege by using the least privileged database user possible.

In particular, avoid using the 'sa' or 'db-owner'

database users. This does not eliminate SQL injection, but minimizes its impact.

Grant the minimum database access that is necessary for the application.

SQL Injection - Oracle - Time Based (1)

▼ POST https://www.plis.sk/volne/hd/hd_p_DetailByk/z_hd_p_Detailbyk.aspx?zviera=SK000813855036

Alert tags

- POLICY_SEQUENCE =
- [OWASP_2021_A03](#)
- [CWE-89](#)
- [WSTG-v42-INPV-05](#)
- POLICY_DEV_FULL =
- POLICY_QA_STD =
- POLICY_QA_FULL =
- [OWASP_2017_A01](#)

Alert description

SQL injection may be possible.

Other info

The query time is controllable using parameter value
[ZmMGCKz0oBGqIHvHDTBykJiNmDLF7B7OWhSpC
ZBrxHHT1ukyai_vVoqidv9ynho48PWMfgZ3nbLAipt
nrZ30wkKz-
indOADFOKKFRmmRjJCUIC4JkNANnRxLOS6SR68q
RXXGL2ds8RijCZXhtnHySw2 / (SELECT
UTL_INADDR.get_host_name('10.0.0.1') from dual
union SELECT
UTL_INADDR.get_host_name('10.0.0.2') from dual
union SELECT
UTL_INADDR.get_host_name('10.0.0.3') from dual
union SELECT
UTL_INADDR.get_host_name('10.0.0.4') from dual
union SELECT
UTL_INADDR.get_host_name('10.0.0.5') from dual)
], which caused the request to take [13,167]
milliseconds, when the original unmodified query
with value
[ZmMGCKz0oBGqIHvHDTBykJiNmDLF7B7OWhSpC
ZBrxHHT1ukyai_vVoqidv9ynho48PWMfgZ3nbLAipt
nrZ30wkKz-
indOADFOKKFRmmRjJCUIC4JkNANnRxLOS6SR68q
RXXGL2ds8RijCZXhtnHySw2] took [117]

milliseconds.

Request

▼ Request line and header section (402 bytes)

```
POST https://www.plis.sk/volne/hd/
hd_p_DetailByk/z_hd_p_Detailbyk.aspx?
zviera=SK000813855036 HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
content-type: application/x-www-form-
urlencoded
referer: https://www.plis.sk/volne/hd/
hd_p_DetailByk/z_hd_p_Detailbyk.aspx?
zviera=SK000813855036
content-length: 8558
Cookie:
ASP.NET_SessionId=fxz2wlx0wzki4botxzazxsgl
```

► Request body (8558 bytes)

Response

▼ Status line and header section (405 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 13:59:29 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 42633
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY
```

► Response body (42633 bytes)

Parameter

__PREVIOUSPAGE

Attack

```
field: [__PREVIOUSPAGE], value
[ZmMGCKz0oBGqIHvHDTBykJiNmDLF7B70WhSpCZBrx
HHT1ukyai_vVoqidv9ynho48PWMfgZ3nbLAiptnrZ3
0wkKz-
ind0ADFOKKFRmmRJjCUIC4JkNANnRxLOS6SR68qRXX
GL2ds8RijCZXhtnHySw2 / (SELECT
UTL_INADDR.get_host_name('10.0.0.1') from
dual union SELECT
UTL_INADDR.get_host_name('10.0.0.2') from
dual union SELECT
UTL_INADDR.get_host_name('10.0.0.3') from
dual union SELECT
UTL_INADDR.get_host_name('10.0.0.4') from
dual union SELECT
UTL_INADDR.get_host_name('10.0.0.5') from
dual) ]
```

Solution

Do not trust client side input, even if there is client side validation in place.

In general, type check all data on the server side.

If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.

If database Stored Procedures can be used, use them.

Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!

Do not create dynamic SQL queries using simple string concatenation.

Escape all data received from the client.

Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.

Apply the principle of least privilege by using the least privileged database user possible.

In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.

Grant the minimum database access that is necessary for the application.

SQL Injection - SQLite (1)

▼ POST https://www.plis.sk/volne/hd/v_hd_medz_gen_hodn/v_hd_medz_gen_hodn.aspx

Alert tags

- [OWASP_2017_A01](#)
- [OWASP_2021_A03](#)
- [CWE-89](#)
- [WSTG-v42-INPV-05](#)
- POLICY_QA_FULL =

Alert description

SQL injection may be possible.

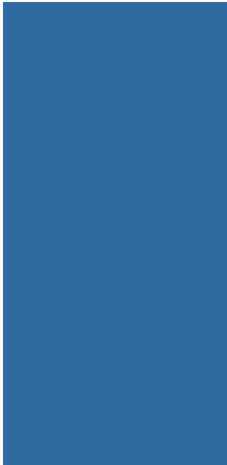
Other info

The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [62] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [6,757] milliseconds, when the original unmodified query with value [tmedF3Udctub]-aalqZhn_b_oHPNj1nrUSaScnsCMkJVsKj2Jkhu4ggg6GhaXHjLzB2MVv9-j0nRjM-BCKszSyl3MmzDRnv05f3fW8qAenKYkmVMqr8PA4IqFFphyM9T03t2fGmM-UfwJjdZdCXefZw2] took [13] milliseconds.

Request

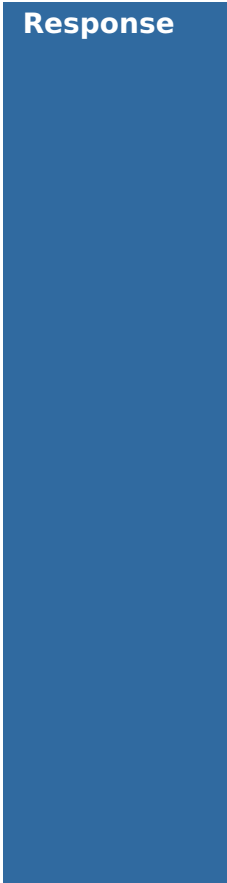
▼ Request line and header section (370 bytes)

```
POST https://www.plis.sk/volne/hd/v_hd_medz_gen_hodn/v_hd_medz_gen_hodn.aspx HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
content-type: application/x-www-form-urlencoded
```



referer: https://www.plis.sk/volne/hd/
v_hd_medz_gen_hodn/
v_hd_medz_gen_hodn.aspx
content-length: 4158
Cookie:
ASP.NET_SessionId=fxz2wlx0wzki4botxzazxsg
l

► Request body (4158 bytes)



Response

▼ Status line and header section (405 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 14:09:25 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 25285
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (25285 bytes)

Parameter

__PREVIOUSPAGE

Attack

case randomblob(10000000) when not null
then 1 else 1 end

Evidence

The query time is controllable using
parameter value [case
randomblob(10000000) when not null then
1 else 1 end], which caused the request
to take [62] milliseconds, parameter
value [case randomblob(100000000) when
not null then 1 else 1 end], which
caused the request to take [6,757]
milliseconds, when the original

unmodified query with value
[tmedF3UdctubJ-
aalqZhn_bHPNj1nrUSaScnsCMkJVsKj2Jkhu4ggg
6GhaXHjLzB2MVv9-j0nRjM-
BCKszSyI3MmzDRnv05f3fw8qAenKYkmVMqr8PA4lq
FFphyM9T03t2fGmM-UfwJJdZdCXefZw2] took
[13] milliseconds.

Solution

Do not trust client side input, even if there is client side validation in place.

In general, type check all data on the server side.

If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'

If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.

If database Stored Procedures can be used, use them.

Do **not** concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!

Do not create dynamic SQL queries using simple string concatenation.

Escape all data received from the client.

Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.

Apply the principle of least privilege by using the least privileged database user possible.

In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.

Grant the minimum database access that is necessary for the application.

▼ GET https://www.plis.sk/js/plugins/validation/additional-methods.min.js

Alert tags

- [OWASP_2017_A09](#)
- [CVE-2022-31147](#)
- [CVE-2021-21252](#)
- [OWASP_2021_A06](#)
- [CWE-1395](#)
- [CVE-2021-43306](#)

Alert description

The identified library appears to be vulnerable.

Other info

The identified library jquery-validation, version 1.11.0 is vulnerable.

CVE-2022-31147

CVE-2021-21252

CVE-2021-43306

<https://github.com/jquery-validation/jquery-validation/blob/master/changelog.md#1194--2022-05-19>

<https://github.com/jquery-validation/jquery-validation/commit/5bbd80d27fc6b607d2f7f106c89522051a9fb0dd>

<https://github.com/advisories/GHSA-ffmh-x56j-9rc3>

<https://github.com/jquery-validation/jquery-validation/blob/master/changelog.md#1200--2023-10-10>

<https://github.com/jquery-validation/jquery-validation/blob/master/changelog.md#1193--2021-01-09>

Request

▼ Request line and header section (300 bytes)

```
GET https://www.plis.sk/js/plugins/validation/additional-methods.min.js
HTTP/1.1
host: www.plis.sk
```



user-agent:
pragma: no-cache
cache-control: no-cache
referer: https://www.plis.sk/volne/ovce/
v_ov_plem_hodn_baran/
v_ov_plem_hodn_baran.aspx
Cookie:
ASP.NET_SessionId=fxz2wlx0wzki4botxzazxs
gl

▼ Request body (0 bytes)

Response



▼ Status line and header section (415 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:52:43 GMT
Content-Type: application/javascript
Content-Length: 10734
Connection: keep-alive
Last-Modified: Mon, 12 Nov 2018
06:57:15 GMT
Accept-Ranges: bytes
ETag: "4722bef1547ad41:0"
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (10734 bytes)

Evidence

/*! jQuery Validation Plugin - v1.11.0

Solution

Upgrade to the latest version of the affected library.

Risk=Medium, Confidence=High (1)

<https://www.plis.sk> (1)

Content Security Policy (CSP) Header Not Set (1)

▼ GET https://www.plis.sk

Alert tags

- [CWE-693](#)
- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)

Alert description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Request

▼ Request line and header section (223 bytes)

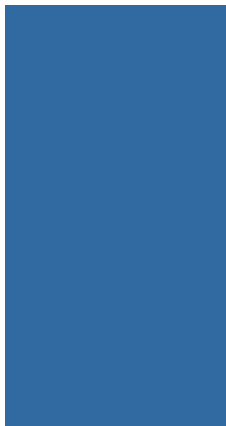
```
GET https://www.plis.sk HTTP/1.1
host: www.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (405 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:53 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 10225
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
```



X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (10225 bytes)

Solution

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Risk=Medium, Confidence=Medium (4)

<https://www.plis.sk> (4)

Multiple X-Frame-Options Header Entries (1)

▼ GET <https://www.plis.sk/login.aspx>

Alert tags

- [WSTG-v42-CLNT-09](#)
- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)
- [CWE-1021](#)

Alert description

X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

Request

▼ Request line and header section (234 bytes)

```
GET https://www.plis.sk/login.aspx
HTTP/1.1
host: www.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```



▼ Request body (0 bytes)



Response

▼ Status line and header section (405 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:53 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 16669
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (16669 bytes)



Parameter

x-frame-options



Solution

Ensure only a single X-Frame-Options header is present in the response.

Potential IP Addresses Found in the Viewstate (1)

▼ POST https://www.plis.sk/volne/kozy/v_ko_ku_ml/v_ko_ku_ml.aspx



Alert tags

- [CWE-642](#)
- [OWASP_2021_A04](#)
- [OWASP_2017_A06](#)



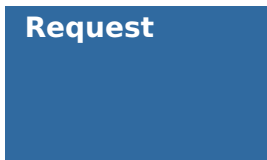
Alert description

The following potential IP addresses were found being serialized in the viewstate field:



Other info

[4.0.0.0]



Request

▼ Request line and header section (342 bytes)

POST https://www.plis.sk/volne/kozy/

v_ko_ku_ml/v_ko_ku_ml.aspx HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
content-type: application/x-www-form-urlencoded
referer: https://www.plis.sk/volne/
kozy/v_ko_ku_ml/v_ko_ku_ml.aspx
content-length: 7806
Cookie:
ASP.NET_SessionId=fxz2wlx0wzki4botxzazx
sgl

► Request body (7806 bytes)

Response

▼ Status line and header section (405 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:59 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 26329
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains;
preload
X-Frame-Options: DENY

► Response body (26329 bytes)

Solution

Verify the provided information isn't confidential.

Secure Pages Include Mixed Content (Including Scripts) (1)

▼ GET https://www.plis.sk/volne/hd/v_hd_naj_chovy/

v_hd_naj_chovy.aspx

Alert tags

- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)
- [WSTG-v42-CRYP-03](#)
- [CWE-311](#)

Alert description

The page includes mixed content, that is content accessed via HTTP instead of HTTPS.

Other info

tag=script src=http://code.jquery.com/jquery-1.9.1.js

tag=script src=http://code.jquery.com/ui/1.10.3/jquery-ui.js

Request

▼ Request line and header section (255 bytes)

```
GET https://www.plis.sk/volne/hd/v_hd_naj_chovy/v_hd_naj_chovy.aspx HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
referer: https://www.plis.sk/volne/hd/hd.aspx
Cookie:
ASP.NET_SessionId=fxz2wlx0wzki4botxzazxsgl
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (405 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:48:00 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 38703
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
```



X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (38703 bytes)

Evidence

<http://code.jquery.com/jquery-1.9.1.js>

Solution

A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS.

The page must not contain any content that is transmitted over unencrypted HTTP.

This includes content from third party sites.

Vulnerable JS Library (1)

▼ GET <https://www.plis.sk/js/jquery.min.js>

Alert tags

- [CVE-2020-11023](#)
- [OWASP_2017_A09](#)
- [CVE-2020-11022](#)
- [OWASP_2021_A06](#)
- [CWE-1395](#)
- [CVE-2015-9251](#)
- [CVE-2019-11358](#)

Alert description

The identified library appears to be vulnerable.

Other info

The identified library jquery, version 1.12.3 is vulnerable.

CVE-2020-11023

CVE-2020-11022

CVE-2015-9251

CVE-2019-11358

<https://github.com/jquery/jquery/issues/2432>

<http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/>

<http://research.insecurelabs.org/jquery/test/>

<https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/>

<https://nvd.nist.gov/vuln/detail/CVE-2019-11358>

<https://github.com/advisories/GHSA-rmxg-73gg-4p98>

<https://nvd.nist.gov/vuln/detail/CVE-2015-9251>

<https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b>

<https://github.com/jquery/jquery.com/issues/162>

<https://bugs.jquery.com/ticket/11974>

<https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/>

Request

▼ Request line and header section (211 bytes)

```
GET https://www.plis.sk/js/jquery.min.js HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
referer: https://www.plis.sk
Cookie:
ASP.NET_SessionId=fllwuvdvh3d0cn15ssgzw3jy
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (415 bytes)

	<p>HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 14 Apr 2025 12:47:55 GMT Content-Type: application/javascript Content-Length: 97185 Connection: keep-alive Last-Modified: Mon, 12 Nov 2018 06:57:13 GMT Accept-Ranges: bytes ETag: "daf7b9f0547ad41:0" X-Powered-By: ASP.NET X-FRAME-OPTIONS: SAMEORIGIN Strict-Transport-Security: max-age=63072000; includeSubdomains; preload X-Frame-Options: DENY</p> <p>► Response body (97185 bytes)</p>
Evidence	/*! jQuery v1.12.3
Solution	Upgrade to the latest version of the affected library.

Risk=Medium, Confidence=Low (1)

<p>https://www.plis.sk (1)</p>	
<p><u>Absence of Anti-CSRF Tokens (1)</u></p>	
<p>▼ GET https://www.plis.sk</p>	
Alert tags	<ul style="list-style-type: none">▪ OWASP_2021_A01▪ WSTG-v42-SESS-05▪ OWASP_2017_A05▪ CWE-352
Alert description	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or</p>

intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- * The victim has an active session on the target site.
- * The victim is authenticated via HTTP auth on the target site.
- * The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Other info

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "__EVENTARGUMENT" "__EVENTTARGET" "__EVENTVALIDATION" "__VIEWSTATE" "__VIEWSTATEGENERATOR"].

Request

▼ Request line and header section (223 bytes)

GET https://www.plis.sk HTTP/1.1

host: www.plis.sk
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache

▼ Request body (0 bytes)

Response

▼ Status line and header section (405 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:53 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 10225
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (10225 bytes)

Evidence

```
<form name="aspnetForm" method="post"
action="." id="aspnetForm">
```

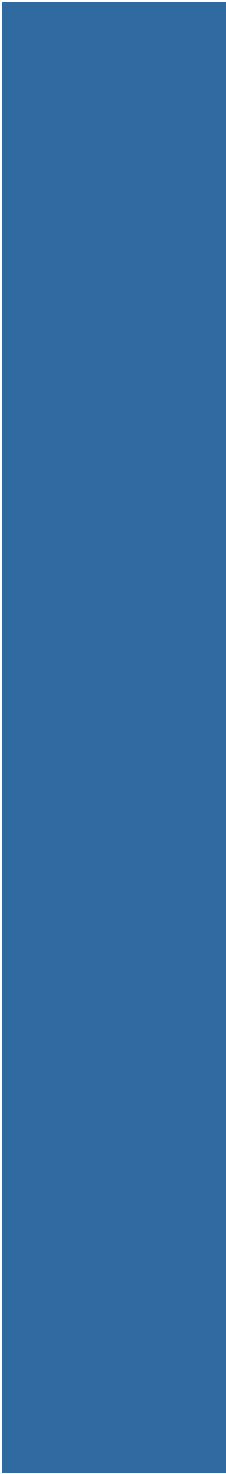
Solution

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation



Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Risk=Low, Confidence=High (3)

<https://api.plis.sk> (2)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▼ GET <https://api.plis.sk/inbreeding/cows/>

Alert tags

- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)
- [WSTG-v42-INFO-02](#)
- [CWE-497](#)

Alert description

The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Request

▼ Request line and header section (240 bytes)

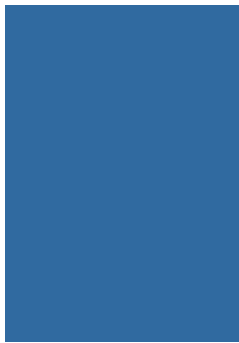
```
GET https://api.plis.sk/inbreeding/cows/
HTTP/1.1
host: api.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (432 bytes)

```
HTTP/1.1 401
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:54 GMT
Content-Type: application/
json; charset=UTF-8
Connection: keep-alive
Set-Cookie:
JSESSIONID=520C4BF3C9C1044335253277B2798D
EF; Path=/; HttpOnly
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-
age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
content-length: 175
```



▼ Response body (175 bytes)

```
{"timestamp":"2025-04-14T12:48:42.253+0000","status":401,"error":"Unauthorized","message":"Full authentication is required to access this resource","path":"/inbreeding/cows/"}
```

Evidence

nginx/1.18.0 (Ubuntu)

Solution

Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.

Strict-Transport-Security Header Not Set (1)

▼ GET https://api.plis.sk/animalInfo/

Alert tags

- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)
- [CWE-319](#)

Alert description

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Request

▼ Request line and header section (235 bytes)

```
GET https://api.plis.sk/animalInfo/
HTTP/1.1
host: api.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (432 bytes)

```
HTTP/1.1 401
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:54 GMT
Content-Type: application/
json;charset=UTF-8
Connection: keep-alive
Set-Cookie:
JSESSIONID=E1EC505BAC744EC9F0DD6363BB8581
61; Path=/; HttpOnly
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-
age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
content-length: 170
```

▼ Response body (170 bytes)

```
{"timestamp":"2025-04-14T12:48:42.165+000
0","status":401,"error":"Unauthorized","m
essage":"Full authentication is required
to access this resource","path":"/
animalInfo/"}
```

Solution

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

<https://www.plis.sk> (1)

X-AspNet-Version Response Header (1)

▼ GET <https://www.plis.sk>

Alert tags

- [WSTG-v42-INFO-08](#)
- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)
- [CWE-933](#)

Alert

Server leaks information via "X-AspNet-

description	Version"/"X-AspNetMvc-Version" HTTP response header field(s).
Other info	An attacker can use this information to exploit known vulnerabilities.
Request	<p>▼ Request line and header section (223 bytes)</p> <pre>GET https://www.plis.sk HTTP/1.1 host: www.plis.sk user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache</pre> <p>▼ Request body (0 bytes)</p>
Response	<p>▼ Status line and header section (405 bytes)</p> <pre>HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 14 Apr 2025 12:47:53 GMT Content-Type: text/html; charset=windows-1250 Content-Length: 10225 Connection: keep-alive Vary: Accept-Encoding Cache-Control: private X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET X-FRAME-OPTIONS: SAMEORIGIN Strict-Transport-Security: max- age=63072000; includeSubdomains; preload X-Frame-Options: DENY</pre> <p>► Response body (10225 bytes)</p>
Evidence	4.0.30319
Solution	Configure the server so it will not return those headers.

<https://api.plis.sk> (2)

Cookie Without Secure Flag (1)

▼ GET <https://api.plis.sk/animalInfo/>

Alert tags

- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)
- [CWE-614](#)
- [WSTG-v42-SESS-02](#)

Alert description

A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Request

▼ Request line and header section (235 bytes)

```
GET https://api.plis.sk/animalInfo/
HTTP/1.1
host: api.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (432 bytes)

```
HTTP/1.1 401
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:54 GMT
Content-Type: application/
json; charset=UTF-8
Connection: keep-alive
Set-Cookie:
JSESSIONID=E1EC505BAC744EC9F0DD6363BB8581
61; Path=/; HttpOnly
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-
```

	age=0, must-revalidate Pragma: no-cache Expires: 0 X-Frame-Options: DENY content-length: 170
	▼ Response body (170 bytes) <pre>{ "timestamp": "2025-04-14T12:48:42.165+0000", "status": 401, "error": "Unauthorized", "message": "Full authentication is required to access this resource", "path": "/animalInfo/" }</pre>
Parameter	JSESSIONID
Evidence	Set-Cookie: JSESSIONID
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

Cookie without SameSite Attribute (1)

▼ GET https://api.plis.sk/animalInfo/

Alert tags	<ul style="list-style-type: none"> ▪ OWASP_2021_A01 ▪ OWASP_2017_A05 ▪ WSTG-v42-SESS-02 ▪ CWE-1275
Alert description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Request	▼ Request line and header section (235 bytes) <pre>GET https://api.plis.sk/animalInfo/ HTTP/1.1 host: api.plis.sk user-agent: Mozilla/5.0 (Windows NT</pre>

10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache

▼ Request body (0 bytes)

Response

▼ Status line and header section (432 bytes)

HTTP/1.1 401
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:54 GMT
Content-Type: application/
json;charset=UTF-8
Connection: keep-alive
Set-Cookie:
JSESSIONID=E1EC505BAC744EC9F0DD6363BB8581
61; Path=/; HttpOnly
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-
age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
content-length: 170

▼ Response body (170 bytes)

```
{"timestamp":"2025-04-14T12:48:42.165+0000", "status":401, "error":"Unauthorized", "message":"Full authentication is required to access this resource", "path":"/animalInfo/"}
```

Parameter

JSESSIONID

Evidence

Set-Cookie: JSESSIONID

Solution

Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Cross-Domain JavaScript Source File Inclusion (1)

▼ GET <https://www.plis.sk/login.aspx>

Alert tags

- [OWASP_2021_A08](#)
- [CWE-829](#)

Alert description

The page includes one or more script files from a third-party domain.

Request

▼ Request line and header section (234 bytes)

```
GET https://www.plis.sk/login.aspx
HTTP/1.1
host: www.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (405 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:53 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 16669
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY
```




► Response body (16669 bytes)

Parameter

https://code.jquery.com/
jquery-3.2.1.min.js

Evidence

```
<script src="https://code.jquery.com/  
jquery-3.2.1.min.js"></script>
```

Solution

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▼ GET https://www.plis.sk

Alert tags

- [OWASP_2021_A01](#)
- [OWASP_2017_A03](#)
- [WSTG-v42-INFO-08](#)
- [CWE-497](#)

Alert description

The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Request

▼ Request line and header section (223 bytes)

```
GET https://www.plis.sk HTTP/1.1  
host: www.plis.sk  
user-agent: Mozilla/5.0 (Windows NT  
10.0; Win64; x64) AppleWebKit/537.36  
(KHTML, like Gecko) Chrome/131.0.0.0  
Safari/537.36  
pragma: no-cache  
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (405 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:53 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 10225
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY
```

► Response body (10225 bytes)

Evidence

X-Powered-By: ASP.NET

Solution

Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

X-Content-Type-Options Header Missing (1)

▼ GET https://www.plis.sk

Alert tags

- [CWE-693](#)
- [OWASP_2021_A05](#)
- [OWASP_2017_A06](#)

Alert description

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Other info

This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scan rule will not alert on client or server error responses.

Request

▼ Request line and header section (223 bytes)

```
GET https://www.plis.sk HTTP/1.1
host: www.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (405 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:53 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 10225
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY
```

► Response body (10225 bytes)

Parameter

x-content-type-options

Solution

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Risk=Low, Confidence=Low (1)

<https://www.plis.sk> (1)

Timestamp Disclosure - Unix (1)

▼ GET <https://www.plis.sk/js/demonstration.min.js>

Alert tags

- [OWASP_2021_A01](#)
- [OWASP_2017_A03](#)
- [CWE-497](#)

Alert description

A timestamp was disclosed by the application/web server. - Unix

Other info

1513671875, which evaluates to: 2017-12-19 08:24:35.

Request

▼ Request line and header section (276 bytes)

```
GET https://www.plis.sk/js/
demonstration.min.js HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
referer: https://www.plis.sk/volne/ovce/
v_ov_plem_hodn_baran/
v_ov_plem_hodn_baran.aspx
Cookie:
ASP.NET_SessionId=fxz2wlx0wzki4botxzazxs
gl
```

	<p>▼ Request body (0 bytes)</p>
Response	<p>▼ Status line and header section (415 bytes)</p> <pre> HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 14 Apr 2025 12:52:45 GMT Content-Type: application/javascript Content-Length: 22964 Connection: keep-alive Last-Modified: Mon, 12 Nov 2018 06:57:13 GMT Accept-Ranges: bytes ETag: "d5a4b2f0547ad41:0" X-Powered-By: ASP.NET X-FRAME-OPTIONS: SAMEORIGIN Strict-Transport-Security: max-age=63072000; includeSubdomains; preload X-Frame-Options: DENY </pre> <p>► Response body (22964 bytes)</p>
Evidence	1513671875
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Risk=Informational, Confidence=High (2)

<p>https://www.plis.sk (2)</p>	
<p><u>Authentication Request Identified (1)</u></p>	
<p>▼ POST https://www.plis.sk/login.aspx</p>	
Alert tags	
Alert description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify

any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.

Other info

userParam=ctl00\$ContentPlaceHolderZabezpVstup\$Login\$LoginButton

userValue=Prihlásiť

passwordParam=ctl00\$ContentPlaceHolderZabezpVstup\$Login\$Password

referer=https://www.plis.sk/login.aspx

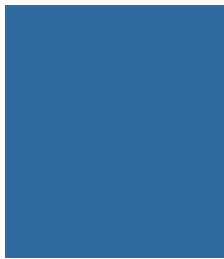
Request

▼ Request line and header section (287 bytes)

```
POST https://www.plis.sk/login.aspx
HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
content-type: application/x-www-form-urlencoded
referer: https://www.plis.sk/login.aspx
content-length: 851
Cookie:
ASP.NET_SessionId=fl1wuvdvh3d0cn15ssgzw3jy
```

▼ Request body (851 bytes)

```
__VIEWSTATE=%2FwEPDwUKMTg1MTY5NDQ2NA9kFgJmD2QWAgIGDxYCHgRocmVmBQ9oZWxwL21hbnVhbC5wZGZlYmYpFgQeA3NyYwUXB2JyYXpreS9tYW51YWwtbGluday5naWYeBmJvcmlcgUBMGQYAUeX19Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgMF0mN0bDAwJENvbnRlbnRQbGFjZUhhbGRlcmlphYmV6cFZzdHVwJExvZ2luJExvZ2luSW1hZ2VCdXR0b24FF2N0bDAwJExvZ2luU3RhZHVzJGN0bDAxBRdjdGwwMCRMb2dpblN0YXR1cyRjdGwwM5WuYPRH47MF0FedUazpzGv4THk2aFBbhjqbxgXEwKl%2B&__VIEWSTATEGENERATOR=C2EE9ABB&__EVENTVALIDATION=%2FwEdAAeyPt2dUR4JwEoGFePq%2BawfLsvIlRf0%2Fthe7635jB5fzkIu4qQ0K81Rh0hrBkkWBnF05MDD8TVYEuE2CHjVfZm6d4DyMymBYHVNjx0E5zMWJAGRv6sgRdYYmxE2xXL23r46YdmBIyo9V6fKNRtUYvB%2F7YYYokR6Igd5vZ45h8eTQw9%2Bi
```



LsiihDMzASqwI7W8%3D&ctl00%24ContentPlaceHolderZabzpvstup%24Login%24UserName=ZAP&ctl00%24ContentPlaceHolderZabzpvstup%24Login%24Password=ZAP&ctl00%24ContentPlaceHolderZabzpvstup%24Login%24LoginButton=Prhl%C3%A1si%C5%A5

Response

▼ Status line and header section (405 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:55 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 12847
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (12847 bytes)

Parameter

ctl00\$ContentPlaceHolderZabzpvstup\$Login\$LoginButton

Evidence

ctl00\$ContentPlaceHolderZabzpvstup\$Login\$Password

Solution

This is an informational alert rather than a vulnerability and so there is nothing to fix.

GET for POST (1)

▼ GET https://www.plis.sk/

Alert tags

- [OWASP_2021_A04](#)
- POLICY_QA_STD =
- POLICY_QA_FULL =
- [WSTG-v42-CONF-06](#)
- [OWASP_2017_A06](#)

	<ul style="list-style-type: none">▪ CWE-16
Alert description	<p>A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.</p>
Request	<p>▼ Request line and header section (734 bytes)</p> <pre>GET https://www.plis.sk/? __EVENTVALIDATION=/ wEdAATWSQlXvUUSpFt8ffxC691XLsvIlRf0/ the7635jB5fzkIu4qQ0K81Rh0hrBkkWBnH46YdmBI yo9V6fKNRtUYvBq036q5VFh7wN70RPDA+ZprriBjX VnRIc3SdWIntXtI8=&__VIEWSTATE=/ wEPDwUKMTAxODY0ODk5NA9kFgJmD2QWAgIGDxYCHg RocmVmBQ9oZWxwL21hbnVhbC5wZGYWAmYPFgQeA3N yYwUXb2JyYXpreS9tYW51YWwtbGluay5naWYeBmJv cmRlcgUBMGQYAUeX19Db250cm9sc1JlcXVpcmVQb 3N0QmFja0tleV9fFgIFF2N0bDAwJExvZ2luU3RhZH VzJGN0bDAxBRdjGwwMCRMb2dpblN0YXR1cyRjdGw wM2YHAEigxTy/sBhqJA4G/ lbxmvsUThPGVhhq1SFuUWkG&__VIEWSTATEGENERA TOR=F9B23BA9 HTTP/1.1 host: www.plis.sk user-agent: pragma: no-cache cache-control: no-cache content-type: application/x-www-form- urlencoded referer: https://www.plis.sk Cookie: ASP.NET_SessionId=fl1wuvdvh3d0cn15ssgzW3j y</pre> <p>▼ Request body (0 bytes)</p>
Response	<p>▼ Status line and header section (404 bytes)</p> <pre>HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 14 Apr 2025 16:18:30 GMT</pre>

Content-Type: text/html;
charset=windows-1250
Content-Length: 9609
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (9609 bytes)

Evidence

GET https://www.plis.sk/?
__EVENTVALIDATION=/
wEdAATWSQlXvUUSpFt8ffxC691XLsvIlRf0/
the7635jB5fzkIu4qQ0K81Rh0hrBkkWBnH46YdmBI
yo9V6fKNRtUYvBq036q5VFh7wN70RPDA+ZprriBjX
VnRIc3SdWIntXtI8=&__VIEWSTATE=/
wEPDwUKMTAxODY0ODk5NA9kFgJmD2QWAgIGDxYCHg
RocmVmBQ9oZWxwL21hbnVhbC5wZGYWAmYPFgQeA3N
yYwUXb2JyYXpreS9tYW51YWwtbGluay5naWYeBmJv
cmRlcgUBMGQYAUeX19Db250cm9sc1JlcXVpcmVQb
3N0QmFja0tleV9fFgIFF2N0bDAwJExvZ2luU3RhdH
VzJGN0bDAxBRdjGwwMCRMb2dpblN0YXR1cyRjdGw
wM2YHAEigxTy/sBhqJA4G/
lbxmvsUThPGVhhq1SFuUWkG&__VIEWSTATEGENERA
TOR=F9B23BA9 HTTP/1.1

Solution

Ensure that only POST is accepted where POST is expected.

Risk=Informational, Confidence=Medium (3)

<https://api.plis.sk> (1)

Session Management Response Identified (1)

▼ GET https://api.plis.sk/animalInfo/

Alert tags

Alert description

The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

Other info

cookie:JSESSIONID

Request

▼ Request line and header section (235 bytes)

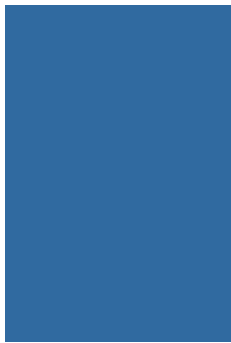
```
GET https://api.plis.sk/animalInfo/
HTTP/1.1
host: api.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (432 bytes)

```
HTTP/1.1 401
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:54 GMT
Content-Type: application/
json;charset=UTF-8
Connection: keep-alive
Set-Cookie:
JSESSIONID=E1EC505BAC744EC9F0DD6363BB8581
61; Path=/; HttpOnly
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-
age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
content-length: 170
```



▼ Response body (170 bytes)

```
{"timestamp": "2025-04-14T12:48:42.165+0000", "status": 401, "error": "Unauthorized", "message": "Full authentication is required to access this resource", "path": "/animalInfo/"}
```

Parameter

JSESSIONID

Evidence

E1EC505BAC744EC9F0DD6363BB858161

Solution

This is an informational alert rather than a vulnerability and so there is nothing to fix.

<https://auth.plis.sk> (1)

User Agent Fuzzer (1)

▼ GET <https://auth.plis.sk/plis/user>

Alert tags

Alert description

Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

Request

▼ Request line and header section (174 bytes)

```
GET https://auth.plis.sk/plis/user
HTTP/1.1
host: auth.plis.sk
user-agent: Mozilla/4.0 (compatible;
MSIE 8.0; Windows NT 6.1)
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (188 bytes)

	<p>HTTP/1.1 405 Server: nginx/1.18.0 (Ubuntu) Date: Mon, 14 Apr 2025 13:02:38 GMT Content-Type: application/ json; charset=UTF-8 Connection: keep-alive Allow: POST content-length: 213</p> <p>▼ Response body (213 bytes)</p> <pre>{ "timestamp": 1744635806888, "status": 405, "error": "Method Not Allowed", "exception": "org.springframework.web.HttpRequestMethodNotSupportedException", "message": "Request method 'GET' not supported", "path": "/plis/user" }</pre>
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

<p>https://www.plis.sk (1)</p> <p>Modern Web Application (1)</p> <p>▼ GET https://www.plis.sk/volne/hd/hd.aspx</p>	
Alert tags	
Alert description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
Other info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Request	<p>▼ Request line and header section (159 bytes)</p> <p>GET https://www.plis.sk/volne/hd/hd.aspx HTTP/1.1</p>

host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
referer: https://www.plis.sk

▼ Request body (0 bytes)

Response

▼ Status line and header section (493 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:54 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 23231
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
Set-Cookie:
ASP.NET_SessionId=fllwuvdvh3d0cn15ssgz3j
y; path=/; HttpOnly; SameSite=Lax
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (23231 bytes)

Evidence

```
<a  
id="ctl00_ContentPlaceHolder1_HyperLink2"  
class="hd_polozky_menu"  
onclick="document.getElementById(&#39;pod  
_ku_ml_kom&#39;).style.display=&#39;none&  
#39;;  
document.getElementById(&#39;ku_ml_kom_cl  
ose&#39;).style.display=&#39;none&#39;;  
document.getElementById(&#39;ku_ml_kom_op  
en&#39;).style.display=&#39;block&#39;;"  
href="#">Kontrola úžitkovosti mliekových  
a kombinovaných plemien</a>
```

Solution

This is an informational alert and so no changes are required.

Risk=Informational, Confidence=Low (4)

<https://www.plis.sk> (4)

Charset Mismatch (Header Versus Meta Charset) (1)

▼ GET https://www.plis.sk/volne/ovce/v_ov_plem_hodn_baran/v_ov_plem_hodn_baran.aspx

Alert tags

- [CWE-436](#)

Alert description

This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.

An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.

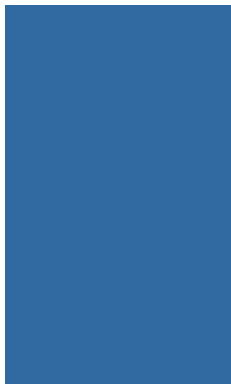
Other info

There was a charset mismatch between the HTTP Header and the META charset encoding declaration: [windows-1250] and [utf-8] do not match.

Request

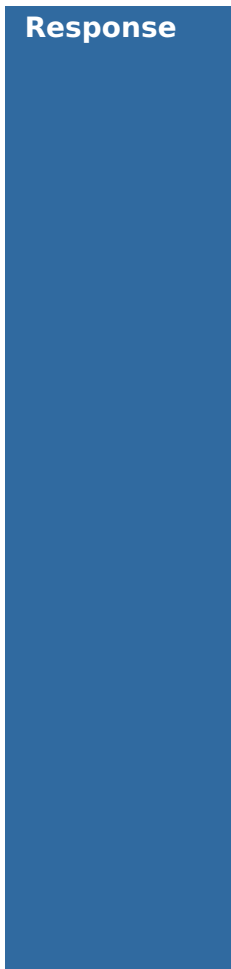
▼ Request line and header section (271 bytes)

```
GET https://www.plis.sk/volne/ovce/
v_ov_plem_hodn_baran/
v_ov_plem_hodn_baran.aspx HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
```



referer: https://www.plis.sk/volne/ovce/ov.aspx
Cookie:
ASP.NET_SessionId=fllwuvdvh3d0cn15ssgzw3jy

▼ Request body (0 bytes)



Response

▼ Status line and header section (447 bytes)

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:59 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 80322
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: no-cache, no-store
Pragma: no-cache
Expires: -1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (80322 bytes)

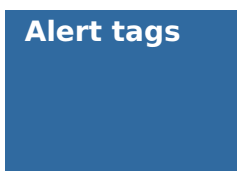


Solution

Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.

Information Disclosure - Suspicious Comments (1)

▼ GET https://www.plis.sk/js/jquery.blockUI.js



Alert tags

- [OWASP_2021_A01](#)
- [WSTG-v42-INFO-05](#)
- [OWASP_2017_A03](#)
- [CWE-615](#)

Alert description

The response appears to contain suspicious comments which may help an attacker.

Other info

The following pattern was used: \bFROM\b and was detected in likely comment: "// be default blockUI will supress tab navigation from leaving blocking content", see evidence field for the suspicious comment/snippet.

Request

▼ Request line and header section (163 bytes)

```
GET https://www.plis.sk/js/
jquery.blockUI.js HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
referer: https://www.plis.sk
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (415 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:54 GMT
Content-Type: application/javascript
Content-Length: 25978
Connection: keep-alive
Last-Modified: Mon, 12 Nov 2018 06:57:13 GMT
Accept-Ranges: bytes
ETag: "50ddb3f0547ad41:0"
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
X-Frame-Options: DENY
```

► Response body (25978 bytes)

Evidence

from

Solution

Remove all comments that return information

that may help an attacker and fix any underlying problems they refer to.

Re-examine Cache-control Directives (1)

▼ GET https://www.plis.sk

Alert tags

- [WSTG-v42-ATHN-06](#)
- [CWE-525](#)

Alert description

The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Request

▼ Request line and header section (223 bytes)

```
GET https://www.plis.sk HTTP/1.1
host: www.plis.sk
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/131.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

Response

▼ Status line and header section (405 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 14 Apr 2025 12:47:53 GMT
Content-Type: text/html;
charset=windows-1250
Content-Length: 10225
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FRAME-OPTIONS: SAMEORIGIN
Strict-Transport-Security: max-
```



age=63072000; includeSubdomains; preload
X-Frame-Options: DENY

► Response body (10225 bytes)

Parameter

cache-control

Evidence

private

Solution

For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

User Controllable HTML Element Attribute (Potential XSS) (1)

▼ POST <https://www.plis.sk/login.aspx>

Alert tags

- [OWASP_2017_A01](#)
- [OWASP_2021_A03](#)
- [CWE-20](#)

Alert description

This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.

Other info

User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:

<https://www.plis.sk/login.aspx>

appears to include user input in:

a(n) [input] tag [value] attribute

The user input found was:

__VIEWSTATEGENERATOR=C2EE9ABB

The user-controlled value was:

c2ee9abb

Request

▼ Request line and header section (287 bytes)

```
POST https://www.plis.sk/login.aspx
HTTP/1.1
host: www.plis.sk
user-agent:
pragma: no-cache
cache-control: no-cache
content-type: application/x-www-form-urlencoded
referer: https://www.plis.sk/login.aspx
content-length: 851
Cookie:
ASP.NET_SessionId=fl1wuvdvh3d0cn15ssgzw3jy
```

▼ Request body (851 bytes)

```
__VIEWSTATE=%2FwEPDwUKMTg1MTY5NDQ2NA9kFgJm
D2QWAgIGDxYCHgRocmVmBQ9oZWxwL21hbnVhbC5wZG
YWAmyPFgQeA3NyYwUXb2JyYXpreS9tYW51YWwtbGlu
ay5naWYeBmJvcmlcgUBMGQYAUeX19Db250cm9sc1
JlcXVpcmVQb3N0QmFja0tleV9fFgMF0mN0bDAwJENv
bnRlbnRQbGFjZUhhbGRlcmlphYmV6cFZzdHVwJExvZ2
luJExvZ2luSW1hZ2VCdXR0b24FF2N0bDAwJExvZ2lu
U3RhdHVzJGN0bDAxBRdjdGwwMCRMb2dpblN0YXR1cy
RjdGwwM5WuYPRH47MF0FedUazpzGv4THk2aFBbhjqb
xgXEwKl%2B&__VIEWSTATEGENERATOR=C2EE9ABB&__
EVENTVALIDATION=%2FwEdAAeyPt2dUR4JwEoGFeP
q%2BawfLsvILRf0%2Fthe7635jB5fzkIu4qQ0K81Rh
0hrBkkWBnF05MDD8TVYEuE2CHjVfZm6d4DyMymBYH
VNjx0E5zMWJAGRv6sgRdYYmxE2xXL23r46YdmBIyo9
V6fKNRtUYvB%2F7YYYokR6Igd5vZ45h8eTQw9%2Bi
LsiihDMzASqwI7W8%3D&ctl00%24ContentPlaceHo
lderZabezpVstup%24Login%24UserName=ZAP&ctl
00%24ContentPlaceHolderZabezpVstup%24Login
%24Password=ZAP&ctl00%24ContentPlaceHolder
ZabezpVstup%24Login%24LoginButton=Prihl%C3
%A1si%C5%A5
```

Response

▼ Status line and header section (405 bytes)

```
HTTP/1.1 200 OK
```

	<div>Server: nginx/1.18.0 (Ubuntu) Date: Mon, 14 Apr 2025 12:47:55 GMT Content-Type: text/html; charset=windows-1250 Content-Length: 12847 Connection: keep-alive Vary: Accept-Encoding Cache-Control: private X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET X-FRAME-OPTIONS: SAMEORIGIN Strict-Transport-Security: max-age=63072000; includeSubdomains; preload X-Frame-Options: DENY</div> <div>► Response body (12847 bytes)</div>
Parameter	__VIEWSTATEGENERATOR
Solution	Validate all input and sanitize output it before writing to any HTML attributes.

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)
CWE ID	359
WASC ID	13

SQL Injection

Source	raised by an active scanner (SQL Injection)
--------	---

CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none"> ▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - MsSQL

Source	raised by an active scanner (SQL Injection - MsSQL)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none"> ▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - Oracle - Time Based

Source	raised by an active scanner (SQL Injection - Oracle)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none"> ▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

SQL Injection - SQLite

Source	raised by an active scanner (SQL Injection - SQLite)
CWE ID	89
WASC ID	19
Reference	<ul style="list-style-type: none"> ▪ https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
---------------	--

CWE ID	1395
Reference	<ul style="list-style-type: none"> ▪ https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	<ul style="list-style-type: none"> ▪ https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html ▪ https://cwe.mitre.org/data/definitions/352.html

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none"> ▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy ▪ https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp ▪ https://caniuse.com/#feat=contentsecuritypolicy ▪ https://content-security-policy.com/

Multiple X-Frame-Options Header Entries

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021
WASC ID	15
Reference	▪ https://tools.ietf.org/html/rfc7034

Potential IP Addresses Found in the Viewstate

Source	raised by a passive scanner (Viewstate)
CWE ID	642
WASC ID	14

Secure Pages Include Mixed Content (Including Scripts)

Source	raised by a passive scanner (Secure Pages Include Mixed Content)
CWE ID	311
WASC ID	4
Reference	▪ https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	1395
Reference	▪ https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Cookie Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
--------	--

CWE ID	614
WASC ID	13
Reference	<ul style="list-style-type: none"> ▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	<ul style="list-style-type: none"> ▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829
WASC ID	15

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source	raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
CWE ID	497
WASC ID	13
Reference	<ul style="list-style-type: none"> ▪ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework



- <https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html>

Server Leaks Version Information via "Server" HTTP Response Header Field

Source

raised by a passive scanner ([HTTP Server Response Header](#))

CWE ID

[497](#)

WASC ID

13

Reference

- <https://httpd.apache.org/docs/current/mod/core.html#servertokens>
- [https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552\(v=pandp.10\)](https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10))
- <https://www.troyhunt.com/shhh-dont-let-your-response-headers/>

Strict-Transport-Security Header Not Set

Source

raised by a passive scanner ([Strict-Transport-Security Header](#))

CWE ID

[319](#)

WASC ID

15

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
- <https://owasp.org/www-community/Security-Headers>
- https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- <https://caniuse.com/stricttransportsecurity>
- <https://datatracker.ietf.org/doc/html/rfc6797>

Timestamp Disclosure - Unix

Source	raised by a passive scanner (Timestamp Disclosure)
CWE ID	497
WASC ID	13
Reference	<ul style="list-style-type: none"> ▪ https://cwe.mitre.org/data/definitions/200.html

X-AspNet-Version Response Header

Source	raised by a passive scanner (X-AspNet-Version Response Header)
CWE ID	933
WASC ID	14
Reference	<ul style="list-style-type: none"> ▪ https://www.troyhunt.com/shhh-dont-let-your-response-headers/ ▪ https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	<ul style="list-style-type: none"> ▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) ▪ https://owasp.org/www-community/Security_Headers

Authentication Request Identified

Source	raised by a passive scanner (Authentication Request Identified)
---------------	---

Reference

- <https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/>

Charset Mismatch (Header Versus Meta Charset)

Source

raised by a passive scanner ([Charset Mismatch](#))

CWE ID

[436](#)

WASC ID

15

Reference

- https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

GET for POST

Source

raised by an active scanner ([GET for POST](#))

CWE ID

[16](#)

WASC ID

20

Information Disclosure - Suspicious Comments

Source

raised by a passive scanner ([Information Disclosure - Suspicious Comments](#))

CWE ID

[615](#)

WASC ID

13

Modern Web Application

Source

raised by a passive scanner ([Modern Web Application](#))

Re-examine Cache-control Directives

Source

raised by a passive scanner ([Re-examine Cache-control Directives](#))

CWE ID

[525](#)

WASC ID

13

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control>
- <https://grayduck.mn/2021/09/13/cache-control-recommendations/>

Session Management Response Identified

Source

raised by a passive scanner ([Session Management Response Identified](#))

Reference

- <https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id>

User Agent Fuzzer

Source

raised by an active scanner ([User Agent Fuzzer](#))

Reference

- <https://owasp.org/wstg>

User Controllable HTML Element Attribute (Potential XSS)

Source

raised by a passive scanner ([User Controllable HTML Element Attribute \(Potential XSS\)](#))

CWE ID

[20](#)

WASC ID

20

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html