acunetix

Developer Report

Acunetix Security Audit

13 March 2023

Generated by Acunetix

Target - http://www.cmcscollege.ac.in/

Scan details

Scan information	
Start url	http://www.cmcscollege.ac.in/
Host	http://www.cmcscollege.ac.in/

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	41
High	2
Medium	24
Low	7
Informational	8

Alerts summary

SQL injection

Classification	
CVSS2	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 10.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-89

Affected items	Variation
Web Server	2

ASP.NET error message

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-16

Affected items	Variation
Web Server	1

Application error message

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	4
/alumini.aspx	2
/ScriptResource.axd	1
/teacherprofile.aspx	1
/WebResource.axd	1

Error message on page

Classification

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/Ev6FQbpDof.aspx	1
/ScriptResource.axd	1
/WebResource.axd	1
/|~.aspx	1

Unencrypted __VIEWSTATE parameter

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1
/Auditorium.aspx	1
/Default.aspx	1
/news.aspx	1
/news/43/avishkar-competition-2022-23.aspx	1
/news/44/satyashodhak-movement.aspx	1
/news/45/phd-admission-2022-23.aspx	1
/pageinfo.aspx	1

Vulnerable Javascript library

Classification	
CVSS2	Base Score: 6.4 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 6.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: Low Availability Impact: None
CWE	CWE-16

Affected items	Variation
/js/jquery.js	1
/js/jquery.min.js	1

ASP.NET version disclosure

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

Affected items	Variation
Web Server	1

Cookie(s) without Secure flag set

Classification

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Session token in URL

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/news.aspx	1

Stack Trace Disclosure (ASP.NET)

Classification

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-209

Affected items	Variation
Web Server	1
/|~.aspx	1

ⓘ Unencrypted connection

Classification	
CVSS2	Base Score: 5.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 9.1 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: High Availability Impact: None
CWE	CWE-310

Affected items	Variation
Web Server	1

ⓘ Content Security Policy (CSP) not implemented

Classification

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

ⓘ Email address found

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/Grievances-Redressal-Cell.aspx	1
/Health-center.aspx	1
/Linkages.aspx	1

ⓘ Error page web server version disclosure

Classification

CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1

Microsoft IIS version disclosure

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation

Web Server	1

Possible username or password disclosure

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/font-awesome-4.3.0/font-awesome-4.3.0/css/font-awesome.css	1

Web Application Firewall detected

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined

CVSS3	Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CWE	CWE-16

Affected items	Variation
Web Server	1

Alerts details

SQL injection

Severity	**High**
Reported by module	/Scripts/PerScheme/Sql_Injection.script

Description

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

Recommendation

Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

References

SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection/)
Types of SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection2/)
Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix (https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/)
SQL Injection - OWASP (https://www.owasp.org/index.php/SQL_Injection)
Bobby Tables: A guide to preventing SQL injection (https://bobby-tables.com/)
SQL Injection Cheet Sheets - Pentestmonkey (http://pentestmonkey.net/category/cheat-sheet/sql-injection)

Affected items

Web Server

Details

Path Fragment input **/<s>/[*].aspx** was set to **@@jXFr6**

Error message found:

```
System.Data.SqlClient.SqlException:
```

Request headers

```
GET /facultyprofile/@@jXFr6.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=axjsse450vdwjl45mvj1oy55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server

Details

Path Fragment input **/<s>/[*]/<s>** was set to @@**qfqpy**

Error message found:

```
System.Data.SqlClient.SqlException:
```

Request headers

```
GET /photo/@@qfqpy/library HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=axjsse450vdwjl45mvj1oy55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

ASP.NET error message

Severity	**Medium**
Reported by module	/Scripts/PerServer/ASP_NET_Error_Message.script

Description

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error message that may disclose sensitive information. By requesting a specially crafted URL, Acunetix generated an ASP.NET error message. The message contains a complete stack trace and Microsoft .NET Framework version.

Impact

Application error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Adjust the application's `web.config` to enable custom errors for remote clients (refer to 'Detailed information' section).

References

customErrors Element (ASP.NET Settings Schema) (https://docs.microsoft.com/en-us/previous-versions/dotnet/netframework-3.0/h0hfz6fc(v=vs.85))

Affected items

Web Server

Details

Error message pattern found:

```
<title>Illegal characters in path.</title>
```

Request headers

```
GET /|~.aspx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Application error message

Severity	**Medium**
Reported by module	/Scripts/PerScheme/XSS.script

Description

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

Web Server

Details

Path Fragment input **/<s>/[*].aspx** was set to
acu10224%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10224

Pattern found:

```
System.Data.SqlClient.SqlException:
```

Request headers

```
GET /facultyprofile/acu10224%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10224.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=axjsse450vdwjl45mvj1oy55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server

Details

Path Fragment input **/<s>/[*]/<s>** was set to **acu1773%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca1773**

Pattern found:

```
System.Data.SqlClient.SqlException:
```

Request headers

```
GET /photo/acu1773%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca1773/library HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=axjsse450vdwjl45mvj1oy55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server

Details

Path Fragment input **/[*].aspx** was set to **SGJUdTllRHl3Rg==**

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
GET /acu10295%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10295.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=axjsse450vdwjl45mvj1oy55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Server

Details

Path Fragment input **/[*]/<n>.aspx** was set to **acu6136%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6136**

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
GET /acu6136%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca6136/15.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=axjsse450vdwjl45mvj1oy55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/ScriptResource.axd

Details

URL encoded GET input **d** was set to **12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'ð¡**

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
GET /ScriptResource.axd?d=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'□&t=ffffffff934f7aa9
HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/WebResource.axd

Details

URL encoded GET input **d** was set to **12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'ð¡**

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
GET /WebResource.axd?d=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'&t=637811689420000000
HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/alumini.aspx

Details

URL encoded POST input **ctl00$ContentPlaceHolder1$ddlyrofjoining** was set to **12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'ð¡**

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
POST /alumini.aspx?PageId=29 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 7058
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

```
__EVENTARGUMENT=1&__EVENTTARGET=1&__EVENTVALIDATION=/wEWgAECtoCZlQYCheLd2wwCtMO4mg0CiOPM9
wcCxoyruQECxoyH4gkCxoyTTwLGjO%2BrDwLbm5GDDALbm%2B3vBALbm7mHBgLbm5XgDgLbm%2BHMBQLbm/2pDALb
m8mSCwLbm6X/AwLbm7HYCgLbm42FAQKwor%2BcBgKwoov5DgKwoqeQCAKworN9ArCij6YPArCim4MGArCi9%2B8OA
rCiw8gFArCi37UMArCiq54LAvTBwugOAvTB3tUFAvTB6mwC9MHGyQ8C9MHSsgYC9MGunw0C9MG6%2BAUC9MGWpQwC
9MHigQsC9MH%2B6gMCyejgRQLJ6PyuDwLJ6IjGCgLJ6OSiAQLJ6PCPCALJ6MxoAsno2NUPAsnotL4GAsnogJsNAsn
onMQFAv6CoIMPAv6CvOwHAv6CyIcBAv6CpOAJAv6CsE0C/oKMtg8C/oKYkwYC/oL0/w4C/oLA2AUC/oLchQwCvdWi
igYC87rFRALzuumfCALzuv2yAQLzuoHWDgLurf/%2BDQLurYOSBQLurdf6BwLurfudDwLurY%2BxBALurZPUDQLur
afvCgLurcuCAgLurd%2BlCwLureN4AoWU0eEHAoWU5YQPAoWUye0JAoWU3YABAoWU4dsOAoWU9f4HAoWUmZIPAoWU
rbUEAoWUscgNAoWUxeMKAsH3rJUPAsH3sKgEAsH3hJEBAsH3qLQOAsH3vM8HAsH3wOIMAsH31IUEAsH3%2BNgNAsH
3jPwKAsH3kJcCAvzejrgBAvzektMOAvze5rsLAvzeil8C/N6e8gkC/N6ilQEC/N62qA4C/N7awwcC/N7u5gwC/N7y
uQQCy7TO/g4Cy7TSkQYCy7SmegLLtMqdCALLtN6wAQLLtOLLDgLLtPbuBwLLtJqCDwLLtK6lBALLtLL4DQLTq7SRB
QLMq7SRBQLNq7SRBQLOq7SRBQLPq7SRBQLIq7SRBQLJq7SRBQKar9CSDALuqrLCAwLUnp3SAQLMkMALAo%2BUwc4M
AoSG9I4BApLM7ZkDAsO6tpAJ0CKZNcnv0Xy7U0fW7a205UCH2lA=&__VIEWSTATE=/wEPDwUKMTQ4NDAyNTYxNw9k
FgJmD2QWAmYPZBYEAgEPFgIeC18hSXRlbUNvdW50AgEWAgIBD2QWAmYPFQJOUGguRC4gQWRtaXNzaW9uIDIwMjItM
jMgSW50ZXJ2aWV3IGlzIHNjaGVkdWxlZCBvbiA4dGggRmVicnVhcnkgMjAyMyBhdCAwODowMGFtAGQCBg9kFggCAQ
8WAh4JaW5uZXJodG1sBfAMPGRpdiBjbGFzcz0idGFibGUtcmVzcG9uc2l2ZSI%2BCgk8dGFibGUgYm9yZGVyPSIwI
iBjbGFzcz0iY29tbWVyY2UtdGJsIiB3aWR0aD0iMTAwJSI%2BCgkJPHRib2R5PgoJCQk8dHI%2BCgkJCQk8dGg%2B
CgkJCQkJU3IuTm8uPC90aD4KCQkJCTx0aD4KCQkJCQlOYW1lPC90aD4KCQkJCTx0aD4KCQkJCQlQb3N0PC90aD4KC
QkJCTx0aD4KCQkJCQlFZHVjYXRpb248L3RoPgoJCQkJPHRoPgoJCQkJCU9jY3VwYXRpb248L3RoPgoJCQkJPHRoPg
oJCQkJCU1vYmlsZSBObzwvdGg%2BCgkJCTwvdHI%2BCgkJCTx0cj4KCQkJCTx0ZD4KCQkJCQkxPC90ZD4KCQkJCTx
0ZD4KCQkJCQlEci5TLk4uU2hpbmRlPC90ZD4KCQkJCTx0ZD4KCQkJCQlDaGFpcm1hbjwvdGQ%2BCgkJCQk8dGQ%2B
CgkJCQkJTS5TYyhDUyksIFBoRDwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJU2VydmljZTwvdGQ%2BCgkJCQk8dGQ%2BC
gkJCQkJwqA8L3RkPgoJCQk8L3RyPgoJCQk8dHI%2BCgkJCQk8dGQ%2BCgkJCQkJMjwvdGQ%2BCgkJCQk8dGQ%2BCg
kJCQkJQ0EuUHJhc2hhbnQgUi4gS2FkYW08L3RkPgoJCQkJPHRkPgoJCQkJCVZpY2UtIENoYWlybWFuPC90ZD4KCQk
JCTx0ZD4KCQkJCQlNQ29tLCBMTEIsIEFDQSwgTkVULCBTRVQsIERDTDwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJU2Vy
dmljZSwgUHJhY3RpY2luZyBDQTwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJwqA8L3RkPgoJCQk8L3RyPgoJCQk8dHI%2
```

```
BCgkJCQk8dGQ%2BCgkJCQkJMzwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJU2hyaS5TYXJ3YXJ0aCBBbmlsIEJvb2I8L3
RkPgoJCQkJPHRkPgoJCQkJCVNlY3JldGFyeTwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJQkJBLCBMTEI8L3RkPgoJCQk
JPHRkPgoJCQkJCUJ1c2luZXNzPC90ZD4KCQkJCTx0ZD4KCQkJCQnCoDwvdGQ%2BCgkJCTwvdHI%2BCgkJCTx0cj4K
CQkJCTx0ZD4KCQkJCQk0PC90ZD4KCQkJCTx0ZD4KCQkJCQlTbXQuUnVwYWxpIFNhdGlzaCBXYWdoPC90ZD4KCQkJC
Tx0ZD4KCQkJCQlBY2NvdW50cyBJbiBjaGFyZ2U8L3RkPgoJCQkJPHRkPgoJCQkJCUJDUywgTUNBPC90ZD4KCQkJCT
x0ZD4KCQkJCQlTZXJ2aWNlPC90ZD4KCQkJCTx0ZD4KCQkJCQnCoDwvdGQ%2BCgkJCTwvdHI%2BCgkJCTx0cj4KCQk
JCTx0ZD4KCQkJCQk1PC90ZD4KCQkJCTx0ZD4KCQkJCQlTaHJpLk5pa2hpbCBBbXJ1dGthcjwvdGQ%2BCgkJCQk8dG
Q%2BCgkJCQkJTWVtYmVyPC90ZD4KCQkJCTx0ZD4KCQkJCQlCQ29tPC90ZD4KCQkJCTx0ZD4KCQkJCQlCdXNpbmVzc
zwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJwqA8L3RkPgoJCQk8L3RyPgoJCQk8dHI%2BCgkJCQk8dGQ%2BCgkJCQkJNj
wvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJU2hyaS5QcmF2aW4gU29uYXdhbmU8L3RkPgoJCQkJPHRkPgoJCQkJCU1lbWJ
lcjwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJQlNjKENTKSwgTVNjKENTKTwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJQnVz
aW5lc3M8L3RkPgoJCQkJPHRkPgoJCQkJCcKgPC90ZD4KCQkJPC90cj4KCQkJPHRyPgoJCQkJPHRkPgoJCQkJCTc8L
3RkPgoJCQkJPHRkPgoJCQkJCVNocmkuQWJoaW5heSBNYWhhZGlrPC90ZD4KCQkJCTx0ZD4KCQkJCQlNZW1iZXI8L3
RkPgoJCQkJPHRkPgoJCQkJCUJDQTwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJQnVzaW5lc3M8L3RkPgoJCQkJPHRkPgo
JCQkJCcKgPC90ZD4KCQkJPC90cj4KCQk8L3Rib2R5PgoJPC90YWJsZT4KPC9kaXY%2BCjxwPgoJwqA8L3A%2BCmQC
BA8QZA8WN2YCAQICAgMCBAIFAgYCBwIIAgkCCgILAgwCDQIOAg8CEAIRAhICEwIUAhUCFgIXAhgCGQIaAhsCHAIdA
h4CHwIgAiECIgIjAiQCJQImAicCKAIpAioCKwIsAi0CLgIvAjACMQIyAjMCNAI1AjYWNxAFBlNlbGVjdAUBMGcQBQ
QyMDIzBQQyMDIzZxAFBDIwMjIFBDIwMjJnEAUEMjAyMQUEMjAyMWcQBQQyMDIwBQQyMDIwZxAFBDIwMTkFBDIwMTl
nEAUEMjAxOAUEMjAxOGcQBQQyMDE3BQQyMDE3ZxAFBDIwMTYFBDIwMTZnEAUEMjAxNQUEMjAxNWcQBQQyMDE0BQQy
MDE0ZxAFBDIwMTMFBDIwMTNnEAUEMjAxMgUEMjAxMmcQBQQyMDExBQQyMDExZxAFBDIwMTAFBDIwMTBnEAUEMjAwO
QUEMjAwOWcQBQQyMDA4BQQyMDA4ZxAFBDIwMDcFBDIwMDdnEAUEMjAwNgUEMjAwNmcQBQQyMDA1BQQyMDA1ZxAFBD
IwMDQFBDIwMDRnEAUEMjAwMwUEMjAwM2cQBQQyMDAyBQQyMDAyZxAFBDIwMDEFBDIwMDFnEAUEMjAwMAUEMjAwMGc
QBQQxOTk5BQQxOTk5ZxAFBDE5OTgFBDE5OThnEAUEMTk5NwUEMTk5N2cQBQQxOTk2BQQxOTk2ZxAFBDE5OTUFBDE5
OTVnEAUEMTk5NAUEMTk5NGcQBQQxOTkzBQQxOTkzZxAFBDE5OTIFBDE5OTJnEAUEMTk5MQUEMTk5MWcQBQQxOTkwB
QQxOTkwZxAFBDE5ODkFBDE5ODlnEAUEMTk4OAUEMTk4OGcQBQQxOTg3BQQxOTg3ZxAFBDE5ODYFBDE5ODZnEAUEMT
k4NQUEMTk4NWcQBQQxOTg0BQQxOTg0ZxAFBDE5ODMFBDE5ODNnEAUEMTk4MgUEMTk4MmcQBQQxOTgxBQQxOTgxZxA
FBDE5ODAFBDE5ODBnEAUEMTk3OQUEMTk3OWcQBQQxOTc4BQQxOTc4ZxAFBDE5NzcFBDE5NzdnEAUEMTk3NgUEMTk3
NmcQBQQxOTc1BQQxOTc1ZxAFBDE5NzQFBDE5NzRnEAUEMTk3MwUEMTk3M2cQBQQxOTcyBQQxOTcyZxAFBDE5NzEFB
DE5NzFnEAUEMTk3MAUEMTk3MGdkZAIGDxBkDxY3ZgIBAgICAwIEAgUCBgIHAggCCQIKAgsCDAINAg4CDwIQAhECEg
ITAhQCFQIWAhcCGAIZAhoCGwIcAh0CHgIfAiACIQIiAiMCJAIlAiYCJwIoAikCKgIrAiwCLQIuAi8CMAIxAjICMwI
0AjUCNhY3EAUGU2VsZWN0BQEwZxAFBDIwMjMFBDIwMjNnEAUEMjAyMgUEMjAyMmcQBQQyMDIxBQQyMDIxZxAFBDIw
MjAFBDIwMjBnEAUEMjAxOQUEMjAxOWcQBQQyMDE4BQQyMDE4ZxAFBDIwMTcFBDIwMTdnEAUEMjAxNgUEMjAxNmcQB
QQyMDE1BQQyMDE1ZxAFBDIwMTQFBDIwMTRnEAUEMjAxMwUEMjAxM2cQBQQyMDEyBQQyMDEyZxAFBDIwMTEFBDIwMT
FnEAUEMjAxMAUEMjAxMGcQBQQyMDA5BQQyMDA5ZxAFBDIwMDgFBDIwMDhnEAUEMjAwNwUEMjAwN2cQBQQyMDA2BQQ
yMDA2ZxAFBDIwMDUFBDIwMDVnEAUEMjAwNAUEMjAwNGcQBQQyMDAzBQQyMDAzZxAFBDIwMDIFBDIwMDJnEAUEMjAw
MQUEMjAwMWcQBQQyMDAwBQQyMDAwZxAFBDE5OTkFBDE5OTlnEAUEMTk5OAUEMTk5OGcQBQQxOTk3BQQxOTk3ZxAFB
DE5OTYFBDE5OTZnEAUEMTk5NQUEMTk5NWcQBQQxOTk0BQQxOTk0ZxAFBDE5OTMFBDE5OTNnEAUEMTk5MgUEMTk5Mm
cQBQQxOTkxBQQxOTkxZxAFBDE5OTAFBDE5OTBnEAUEMTk4OQUEMTk4OWcQBQQxOTg4BQQxOTg4ZxAFBDE5ODcFBDE
5ODdnEAUEMTk4NgUEMTk4NmcQBQQxOTg1BQQxOTg1ZxAFBDE5ODQFBDE5ODRnEAUEMTk4MwUEMTk4M2cQBQQxOTgy
BQQxOTgyZxAFBDE5ODEFBDE5ODFnEAUEMTk4MAUEMTk4MGcQBQQxOTc5BQQxOTc5ZxAFBDE5NzgFBDE5NzhnEAUEM
Tk3NwUEMTk3N2cQBQQxOTc2BQQxOTc2ZxAFBDE5NzUFBDE5NzVnEAUEMTk3NAUEMTk3NGcQBQQxOTczBQQxOTczZx
AFBDE5NzIFBDE5NzJnEAUEMTk3MQUEMTk3MWcQBQQxOTcwBQQxOTcwZ2RkAggPEA8WBh4NRGF0YVRleHRGaWVsZAU
LQ291cnNlc05hbWUeDkRhdGFWYWx1ZUZpZWxkBQhDb3Vyc2VJZB4LXyFEYXRhQm91bmRnZA8WBgIBAgICAwIEAgUC
BhYGEAUGQi5Db20uBQExZxAFBUIuQi5BBQEyZxAFHUIuQi5BLiAoQ29tcHV0ZXIgQXBwbGljYXRpb24pBQEzZxAFG
UIuIFNjLiAoQ29tcHV0ZXIgU2NpZW5jZSkFATRnEAUYTS5TYy4gKENvbXB1dGVyIFNjaWVuY2UpBQE1ZxAFBU0uY2
9tBQE2Z2RkZPanRnt4a5riNZF%2BZdIkdcKzg7Oj&__VIEWSTATEGENERATOR=9B787514&ctl00%24ContentPla
ceHolder1%24btnadd=ADD&ctl00%24ContentPlaceHolder1%24ddlcourse=2&ctl00$ContentPlaceHolder
1$ddlyrofjoining=12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'
&ctl00%24ContentPlaceHolder1%24ddlyrofpassing=0&ctl00%24ContentPlaceHolder1%24hdnPageId=2
9&ctl00%24ContentPlaceHolder1%24txtcode=94102&ctl00%24ContentPlaceHolder1%24txtcomment=55
5&ctl00%24ContentPlaceHolder1%24txtdesign=555&ctl00%24ContentPlaceHolder1%24txtemail=samp
le%40email.tst&ctl00%24ContentPlaceHolder1%24txtmobile=987-65-
4329&ctl00%24ContentPlaceHolder1%24txtname=ncMUFCMU&ctl00%24ContentPlaceHolder1%24txtoffi
ceaddress=3137%20Laguna%20Street&ctl00%24ContentPlaceHolder1%24txtphone=555-666-0606
```

/alumini.aspx

Details

URL encoded POST input **ctl00$ContentPlaceHolder1$ddlyrofpassing** was set to **12345'"\'\");|]*%00{%0d%0a<%00>%bf%27'ð¡**

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
POST /alumini.aspx?PageId=29 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 7058
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

```
__EVENTARGUMENT=1&__EVENTTARGET=1&__EVENTVALIDATION=/wEWgAECtoCZlQYCheLd2wwCtMO4mg0CiOPM9
wcCxoyruQECxoyH4gkCxoyTTwLGjO%2BrDwLbm5GDDALbm%2B3vBALbm7mHBgLbm5XgDgLbm%2BHMBQLbm/2pDALb
m8mSCwLbm6X/AwLbm7HYCgLbm42FAQKwor%2BcBgKwoov5DgKwoqeQCAKworN9ArCij6YPArCim4MGArCi9%2B8OA
rCiw8gFArCi37UMArCiq54LAvTBwugOAvTB3tUFAvTB6mwC9MHGyQ8C9MHSsgYC9MGunw0C9MG6%2BAUC9MGWpQwC
9MHigQsC9MH%2B6gMCyejgRQLJ6PyuDwLJ6IjGCgLJ6OSiAQLJ6PCPCALJ6MxoAsno2NUPAsnotL4GAsnogJsNAsn
onMQFAv6CoIMPAv6CvOwHAv6CyIcBAv6CpOAJAv6CsE0C/oKMtg8C/oKYkwYC/oL0/w4C/oLA2AUC/oLchQwCvdWi
igYC87rFRALzuumfCALzuv2yAQLzuoHWDgLurf/%2BDQLurYOSBQLurdf6BwLurfudDwLurY%2BxBALurZPUDQLur
afvCgLurcuCAgLurd%2BlCwLureN4AoWU0eEHAoWU5YQPAoWUye0JAoWU3YABAoWU4dsOAoWU9f4HAoWUmZIPAoWU
rbUEAoWUscgNAoWUxeMKAsH3rJUPAsH3sKgEAsH3hJEBAsH3qLQOAsH3vM8HAsH3wOIMAsH31IUEAsH3%2BNgNAsH
3jPwKAsH3kJcCAvzejrgBAvzektMOAvze5rsLAvzeil8C/N6e8gkC/N6ilQEC/N62qA4C/N7awwcC/N7u5gwC/N7y
uQQCy7TO/g4Cy7TSkQYCy7SmegLLtMqdCALLtN6wAQLLtOLLDgLLtPbuBwLLtJqCDwLLtK6lBALLtLL4DQLTq7SRB
QLMq7SRBQLNq7SRBQLOq7SRBQLPq7SRBQLIq7SRBQLJq7SRBQKar9CSDALuqrLCAwLUnp3SAQLMkMALAo%2BUwc4M
AoSG9I4BApLM7ZkDAsO6tpAJ0CKZNcnv0Xy7U0fW7a205UCH2lA=&__VIEWSTATE=/wEPDwUKMTQ4NDAyNTYxNw9k
FgJmD2QWAmYPZBYEAgEPFgIeC18hSXRlbUNvdW50AgEWAgIBD2QWAmYPFQJOUGguRC4gQWRtaXNzaW9uIDIwMjItM
jMgSW50ZXJ2aWV3IGlzIHNjaGVkdWxlZCBvbiA4dGggRmVicnVhcnkgMjAyMyBhdCAwODowMGFtAGQCBg9kFggCAQ
8WAh4JaW5uZXJodG1sBfAMPGRpdiBjbGFzcz0idGFibGUtcmVzcG9uc2l2ZSI%2BCgk8dGFibGUgYm9yZGVyPSIwI
iBjbGFzcz0iY29tbWVyY2UtdGJsIiB3aWR0aD0iMTAwJSI%2BCgkJPHRib2R5PgoJCQk8dHI%2BCgkJCQk8dGg%2B
CgkJCQkJU3IuTm8uPC90aD4KCQkJCTx0aD4KCQkJCQlOYW1lPC90aD4KCQkJCTx0aD4KCQkJCQlQb3N0PC90aD4KC
QkJCTx0aD4KCQkJCQlFZHVjYXRpb248L3RoPgoJCQkJPHRoPgoJCQkJCU9jY3VwYXRpb248L3RoPgoJCQkJPHRoPg
oJCQkJCU1vYmlsZSBObzwvdGg%2BCgkJCTwvdHI%2BCgkJCTx0cj4KCQkJCTx0ZD4KCQkJCQkxPC90ZD4KCQkJCTx
0ZD4KCQkJCQlEci5TLk4uU2hpbmRlPC90ZD4KCQkJCTx0ZD4KCQkJCQlDaGFpcm1hbjwvdGQ%2BCgkJCQk8dGQ%2B
CgkJCQkJTS5TYyhDUyksIFBoRDwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJU2VydmljZTwvdGQ%2BCgkJCQk8dGQ%2BC
gkJCQkJwqA8L3RkPgoJCQk8L3RyPgoJCQk8dHI%2BCgkJCQk8dGQ%2BCgkJCQkJMjwvdGQ%2BCgkJCQk8dGQ%2BCg
kJCQkJQ0EuUHJhc2hhbnQgUi4gS2FkYW08L3RkPgoJCQkJPHRkPgoJCQkJCVZpY2UtIENoYWlybWFuPC90ZD4KCQk
JCTx0ZD4KCQkJCQlNQ29tLCBMTEIsIEFDQSwgTkVULCBTRVQsIERDTDwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJU2Vy
dmljZSwgUHJhY3RpY2luZyBDQTwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJwqA8L3RkPgoJCQk8L3RyPgoJCQk8dHI%2
BCgkJCQk8dGQ%2BCgkJCQkJMzwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJU2hyaS5TYXJ3YXJ0aCBBbmlsIEJvb2I8L3
RkPgoJCQkJPHRkPgoJCQkJCVNlY3JldGFyeTwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJQkJBLCBMTEI8L3RkPgoJCQk
JPHRkPgoJCQkJCUJ1c2luZXNzPC90ZD4KCQkJCTx0ZD4KCQkJCQnCoDwvdGQ%2BCgkJCTwvdHI%2BCgkJCTx0cj4K
CQkJCTx0ZD4KCQkJCQk0PC90ZD4KCQkJCTx0ZD4KCQkJCQlTbXQuUnVwYWxpIFNhdGlzaCBXYWdoPC90ZD4KCQkJC
Tx0ZD4KCQkJCQlBY2NvdW50cyBJbiBjaGFyZ2U8L3RkPgoJCQkJPHRkPgoJCQkJCUJDUywgTUNBPC90ZD4KCQkJCTx0ZD4KCQkJCQlTZXJ2aWNlPC90ZD4KCQkJCTx0ZD4KCQkJCQnCoDwvdGQ%2BCgkJCTwvdHI%2BCgkJCTx0cj4KCQk
JCTx0ZD4KCQkJCQk1PC90ZD4KCQkJCTx0ZD4KCQkJCQlTaHJpLk5pa2hpbCBBbXJ1dGhcjwvdGQ%2BCgkJCQk8dG
Q%2BCgkJCQkJTWVtYmVyPC90ZD4KCQkJCTx0ZD4KCQkJCQlCQ29tPC90ZD4KCQkJCTx0ZD4KCQkJCQlCdXNpbmVzc
zwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJwqA8L3RkPgoJCQk8L3RyPgoJCQk8dHI%2BCgkJCQk8dGQ%2BCgkJCQkJNj
wvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJU2hyaS5QcmF2aW4gU29uYXdhbmU8L3RkPgoJCQkJPHRkPgoJCQkJCU1lbWJ
lcjwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJQlNjKENTKSwgTVNjKENTKTwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJQnVz
aW5lc3M8L3RkPgoJCQkJPHRkPgoJCQkJCcKgPC90ZD4KCQkJPC90cj4KCQkJPHRyPgoJCQkJPHRkPgoJCQkJCTc8L
3RkPgoJCQkJPHRkPgoJCQkJCVNocmkuQWJoaW5heSBNYWhhZGlrPC90ZD4KCQkJCTx0ZD4KCQkJCQlNZW1iZXI8L3
RkPgoJCQkJPHRkPgoJCQkJCUJDQTwvdGQ%2BCgkJCQk8dGQ%2BCgkJCQkJQnVzaW5lc3M8L3RkPgoJCQkJPHRkPgo
```

```
JCQkJCcKgPC90ZD4KCQkJPC90cj4KCQk8L3Rib2R5PgoJPC90YWJsZT4KPC9kaXY%2BCjxwPgoJwqA8L3A%2BCmQC
BA8QZA8WN2YCAQICAgMCBAIFAgYCBwIIAgkCCgILAgwCDQIOAg8CEAIRAhICEwIUAhUCFgIXAhgCGQIaAhsCHAIdA
h4CHwIgAiECIgIjAiQCJQImAicCKAIpAioCKwIsAi0CLgIvAjACMQIyAjMCNAI1AjYWNxAFBlNlbGVjdAUBMGcQBQ
QyMDIzBQQyMDIzZxAFBDIwMjIFBDIwMjJnEAUEMjAyMQUEMjAyMWcQBQQyMDIwBQQyMDIwZxAFBDIwMTkFBDIwMTl
nEAUEMjAxOAUEMjAxOGcQBQQyMDE3BQQyMDE3ZxAFBDIwMTYFBDIwMTZnEAUEMjAxNQUEMjAxNWcQBQQyMDE0BQQy
MDE0ZxAFBDIwMTMFBDIwMTNnEAUEMjAxMgUEMjAxMmcQBQQyMDExBQQyMDExZxAFBDIwMTAFBDIwMTBnEAUEMjAwO
QUEMjAwOWcQBQQyMDA4BQQyMDA4ZxAFBDIwMDcFBDIwMDdnEAUEMjAwNgUEMjAwNmcQBQQyMDA1BQQyMDA1ZxAFBD
IwMDQFBDIwMDRnEAUEMjAwMwUEMjAwM2cQBQQyMDAyBQQyMDAyZxAFBDIwMDEFBDIwMDFnEAUEMjAwMAUEMjAwMGc
QBQQxOTk5BQQxOTk5ZxAFBDE5OTgFBDE5OThnEAUEMTk5NwUEMTk5N2cQBQQxOTk2BQQxOTk2ZxAFBDE5OTUFBDE5
OTVnEAUEMTk5NAUEMTk5NGcQBQQxOTkzBQQxOTkzZxAFBDE5OTIFBDE5OTJnEAUEMTk5MQUEMTk5MWcQBQQxOTkwB
QQxOTkwZxAFBDE5ODkFBDE5ODlnEAUEMTk4OAUEMTk4OGcQBQQxOTg3BQQxOTg3ZxAFBDE5ODYFBDE5ODZnEAUEMT
k4NQUEMTk4NWcQBQQxOTg0BQQxOTg0ZxAFBDE5ODMFBDE5ODNnEAUEMTk4MgUEMTk4MmcQBQQxOTgxBQQxOTgxZxA
FBDE5ODAFBDE5ODBnEAUEMTk3OQUEMTk3OWcQBQQxOTc4BQQxOTc4ZxAFBDE5NzcFBDE5NzdnEAUEMTk3NgUEMTk3
NmcQBQQxOTc1BQQxOTc1ZxAFBDE5NzQFBDE5NzRnEAUEMTk3MwUEMTk3M2cQBQQxOTcyBQQxOTcyZxAFBDE5NzEFB
DE5NzFnEAUEMTk3MAUEMTk3MGdkZAIGDxBkDxY3ZgIBAgICAwIEAgUCBgIHAggCCQIKAgsCDAINAg4CDwIQAhECEg
ITAhQCFQIWAhcCGAIZAhoCGwIcAh0CHgIfAiACIQIiAiMCJAIlAiYCJwIoAikCKgIrAiwCLQIuAi8CMAIxAjICMwI
0AjUCNhY3EAUGU2VsZWN0BQEwZxAFBDIwMjMFBDIwMjNnEAUEMjAyMgUEMjAyMmcQBQQyMDIxBQQyMDIxZxAFBDIw
MjAFBDIwMjBnEAUEMjAxOQUEMjAxOWcQBQQyMDE4BQQyMDE4ZxAFBDIwMTcFBDIwMTdnEAUEMjAxNgUEMjAxNmcQB
QQyMDE1BQQyMDE1ZxAFBDIwMTQFBDIwMTRnEAUEMjAxMwUEMjAxM2cQBQQyMDEyBQQyMDEyZxAFBDIwMTEFBDIwMT
FnEAUEMjAxMAUEMjAxMGcQBQQyMDA5BQQyMDA5ZxAFBDIwMDgFBDIwMDhnEAUEMjAwNwUEMjAwN2cQBQQyMDA2BQQ
yMDA2ZxAFBDIwMDUFBDIwMDVnEAUEMjAwNAUEMjAwNGcQBQQyMDAzBQQyMDAzZxAFBDIwMDIFBDIwMDJnEAUEMjAw
MQUEMjAwMWcQBQQyMDAwBQQyMDAwZxAFBDE5OTkFBDE5OTlnEAUEMTk5OAUEMTk5OGcQBQQxOTk3BQQxOTk3ZxAFB
DE5OTYFBDE5OTZnEAUEMTk5NQUEMTk5NWcQBQQxOTk0BQQxOTk0ZxAFBDE5OTMFBDE5OTNnEAUEMTk5MgUEMTk5Mm
cQBQQxOTkxBQQxOTkxZxAFBDE5OTAFBDE5OTBnEAUEMTk4OQUEMTk4OWcQBQQxOTg4BQQxOTg4ZxAFBDE5ODcFBDE
5ODdnEAUEMTk4NgUEMTk4NmcQBQQxOTg1BQQxOTg1ZxAFBDE5ODQFBDE5ODRnEAUEMTk4MwUEMTk4M2cQBQQxOTgy
BQQxOTgyZxAFBDE5ODEFBDE5ODFnEAUEMTk4MAUEMTk4MGcQBQQxOTc5BQQxOTc5ZxAFBDE5NzgFBDE5NzhnEAUEM
Tk3NwUEMTk3N2cQBQQxOTc2BQQxOTc2ZxAFBDE5NzUFBDE5NzVnEAUEMTk3NAUEMTk3NGcQBQQxOTczBQQxOTczZx
AFBDE5NzIFBDE5NzJnEAUEMTk3MQUEMTk3MWcQBQQxOTcwBQQxOTcwZ2RkAggPEA8WBh4NRGF0YVRleHRGaWVsZAU
LQ291cnNlc05hbWUeDkRhdGFWYWx1ZUZpZWxkBQhDb3Vyc2VJZB4LXyFEYXRhQm91bmRnZA8WBgIBAgICAwIEAgUC
BhYGEAUGQi5Db20uBQExZxAFBUIuQi5BBQEyZxAFHUIuQi5BLiAoQ29tcHV0ZXIgQXBwbGljYXRpb24pBQEzZxAFG
UIuIFNjLiAoQ29tcHV0ZXIgU2NpZW5jZSkFATRnEAUYTS5TYy4gKENvbXB1dGVyIFNjaWVuY2UpBQE1ZxAFBU0uY2
9tBQE2Z2RkZPanRnt4a5riNZF%2BZdIkdcKzg7Oj&__VIEWSTATEGENERATOR=9B787514&ctl00%24ContentPla
ceHolder1%24btnadd=ADD&ctl00%24ContentPlaceHolder1%24ddlcourse=2&ctl00%24ContentPlaceHold
er1%24ddlyrofjoining=0&ctl00$ContentPlaceHolder1$ddlyrofpassing=12345'"\'\");|]*%00{%0d%0
a<%00>%bf%27'□
&ctl00%24ContentPlaceHolder1%24hdnPageId=29&ctl00%24ContentPlaceHolder1%24txtcode=94102&c
tl00%24ContentPlaceHolder1%24txtcomment=555&ctl00%24ContentPlaceHolder1%24txtdesign=555&c
tl00%24ContentPlaceHolder1%24txtemail=sample%40email.tst&ctl00%24ContentPlaceHolder1%24tx
tmobile=987-65-
4329&ctl00%24ContentPlaceHolder1%24txtname=ncMUFCMU&ctl00%24ContentPlaceHolder1%24txtoffi
ceaddress=3137%20Laguna%20Street&ctl00%24ContentPlaceHolder1%24txtphone=555-666-0606
```

/teacherprofile.aspx

Details

URL encoded GET input **ProfileId** was set to **acu10008%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10008**

Pattern found:

```
System.Data.SqlClient.SqlException:
```

Request headers

```
GET /teacherprofile.aspx?ProfileId=acu10008%EF%BC%9Cs1%EF%B9%A5s2%CA%BAs3%CA%B9uca10008
HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=axjsse450vdwjl45mvj1oy55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Error message on page

Severity	**Medium**
Reported by module	/Scripts/PerFile/Text_Search_File.script

Description

This alert requires manual confirmation

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.

Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages may disclose sensitive information which can be used to escalate attacks.

Recommendation

Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

PHP Runtime Configuration (https://www.php.net/manual/en/errorfunc.configuration.php#ini.display-errors)
Improper Error Handling (https://www.owasp.org/index.php/Improper_Error_Handling)

Affected items

/Ev6FQbpDof.aspx

Details

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
GET /Ev6FQbpDof.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/ScriptResource.axd

Details

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
GET /ScriptResource.axd HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/WebResource.axd

Details

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
GET /WebResource.axd HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/|~.aspx

Details

Pattern found:

```
ASP.NET is configured to show verbose error messages
```

Request headers

```
GET /|~.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Unencrypted __VIEWSTATE parameter

Severity	**Medium**
Reported by module	/RPA/Unencrypted_VIEWSTATE.js

Description

The __VIEWSTATE parameter is not encrypted. To reduce the chance of someone intercepting the information stored in the ViewState, it is good design to encrypt the ViewState. To do this, set the machineKey validation type to AES. This instructs ASP.NET to encrypt the ViewState value using the Advanced Encryption Standard.

Impact

Possible sensitive information disclosure.

Recommendation

Open **Web.Config** and add the following line under the **<system.web>** element:

```
<machineKey validation="AES"/>
```

Affected items

Web Server

Details

Strings extracted from ViewState (truncated):

1384310407 _!ItemCount NPh.D. Admission 2022-23 Interview is scheduled on 8th February 2023 at 08:00am <div class='item active'>Qhttp://www.cmcscollege.ac.in/img/department/gallary/HomeSlider_20182109034653.jpgd <div class='item'>Qhttp://www.cmcscollege.ac.in/img/department/gallary/HomeSlider_20182109031315.jpgd <div class='item'>Qhttp://www.cmcscollege.ac.in/img/department/gallary/HomeSlider_20182109034704.jpgd

Request headers

```
GET / HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/Auditorium.aspx

Details

Strings extracted from ViewState (truncated):

1368401346 _!ItemCount NPh.D. Admission 2022-23 Interview is scheduled on 8th February 2023 at 08:00am 6http://www.cmcscollege.ac.in/img/slider-auditorium.jpgd class 0col-lg-12 col-md-12 col-sm-12 col-xs-12 pad-LR-0

Request headers

```
GET /Auditorium.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/Default.aspx

Details

Strings extracted from ViewState (truncated):

1384310407 _!ItemCount NPh.D. Admission 2022-23 Interview is scheduled on 8th February 2023 at 08:00am <div class='item active'>Qhttp://www.cmcscollege.ac.in/img/department/gallary/HomeSlider_20182109034653.jpgd <div class='item'>Qhttp://www.cmcscollege.ac.in/img/department/gallary/HomeSlider_20182109031315.jpgd <div class='item'>Qhttp://www.cmcscollege.ac.in/img/department/gallary/HomeSlider_20182109034704.jpgd

Request headers

```
POST /Default.aspx HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 2520
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

__EVENTARGUMENT=1&__EVENTTARGET=1&__VIEWSTATE=/wEPDwUKMTM4NDMxMDQwNw9kFgJmD2QWAmYPZBYEAgE
PFgIeC18hSXRlbUNvdW50AgEWAgIBD2QWAmYPFQJOUGguRC4gQWRtaXNzaW9uIDIwMjItMjMgSW50ZXJ2aWV3IGlz
IHNjaGVkdWxlZCBvbiA4dGggRmVicnVhcnkgMjAyMyBhdCAwODowMGFtAGQCBg9kFgQCAQ8WAh8AAgcWDgIBD2QWA
mYPFQIZPGRpdiBjbGFzcz0naXRlbSBhY3RpdmUnPlFodHRwOi8vd3d3LmNtY3Njb2xsZWdlLmFjLmluL2ltZy9kZX
BhcnRtZW50L2dhbGxhcnkvSG9tZVNsaWRlcl8yMDE4MjEwOTAzNDY1My5qcGdkAgIPZBYCZg8VAhI8ZGl2IGNsYXN
zPSdpdGVtJz5RaHR0cDovL3d3dy5jbWNzY29sbGVnZS5hYy5pbi9pbWcvZGVwYXJ0bWVudC9nYWxsYXJ5L0hvbWVT
bGlkZXJfMjAxODIxMDkwMzEzMTUuanBnZAIDD2QWAmYPFQISPGRpdiBjbGFzcz0naXRlbSc%2BUWh0dHA6Ly93d3c
uY21jc2NvbGxlZ2UuYWMuaW4vaW1nL2RlcGFydG1lbnQvZ2FsbGFyeS9Ib21lU2xpZGVyXzIwMTgyMTA5MDM0NzA0
LmpwZ2QCBA9kFgJmDxUCEjxkaXYgY2xhc3M9J2l0ZW0nPlFodHRwOi8vd3d3LmNtY3Njb2xsZWdlLmFjLmluL2ltZ
y9kZXBhcnRtZW50L2dhbGxhcnkvSG9tZVNsaWRlcl8yMDE4MjEwOTAzMTM0NC5qcGdkAgUPZBYCZg8VAhI8ZGl2IG
NsYXNzPSdpdGVtJz5RaHR0cDovL3d3dy5jbWNzY29sbGVnZS5hYy5pbi9pbWcvZGVwYXJ0bWVudC9nYWxsYXJ5L0h
vbWVTbGlkZXJfMjAxODIxMDkwMzEzNTkuanBnZAIGD2QWAmYPFQISPGRpdiBjbGFzcz0naXRlbSc%2BUWh0dHA6Ly
93d3cuY21jc2NvbGxlZ2UuYWMuaW4vaW1nL2RlcGFydG1lbnQvZ2FsbGFyeS9Ib21lU2xpZGVyXzIwMTkwNzA2MDA
yOTIzLmpwZ2QCBw9kFgJmDxUCEjxkaXYgY2xhc3M9J2l0ZW0nPlFodHRwOi8vd3d3LmNtY3Njb2xsZWdlLmFjLmlu
L2ltZy9kZXBhcnRtZW50L2dhbGxhcnkvSG9tZVNsaWRlcl8yMDIwMjYwMjAxNDQyNi5qcGdkAgMPZBYCZg8WAh8AA
gMWBgIBD2QWAmYPFQMXUGguRC4gQWRtaXNzaW9uIDIwMjItMjOYAUludGVydmlld3MgZm9yIFBoLkQuIGFkbWlzc2
lvbnMgd2lsbCBiZSBoZWxkIG9uIDh0aCBGZWJydWFyeSAyMDIzIGF0IDA4LjAwIGEubS4KCgnCoAoKCUNhbmRpZGF
0ZXMgYXJlIHJlcXVpcmVkIHRvIGJyaW5nIGFsb25nIHdpdGggdGhlbSB0aGUgZm9sbG93aW5nLi4uVzxhIGhyZWY9
aHR0cDovL3d3dy5jbWNzY29sbGVnZS5hYy5pbi9uZXdzLzQ1L3BoZC1hZG1pc3Npb24tMjAyMi0yMy5hc3B4PjxiP
m1vcmU8L2I%2BPC9hPmQCAg9kFgJmDxUDHEF2aXNoa2FyIENvbXBldGl0aW9uIDIwMjItMjOXASJBdmlzaGthciBD
b21wZXRpdGlvbiAyMDIyLTIzIiB3YXMgaGVsZCBpbiBDb2xsZWdlIG9uIDE0dGggU2VwdGVtYmVyIDIwMjIuIEEgd
G90YWwgb2YgNTAgc3R1ZGVudCBncm91cHMgcGFydGljaXBhdGVkIGluIHRoaXMgY29tcGV0aXRpb24uIEluYXVndX
JhdGkuLi5ePGEgaHJlZj1odHRwOi8vd3d3LmNtY3Njb2xsZWdlLmFjLmluL25ld3MvNDMvYXZpc2hrYXItY29tcGV
0aXRpb24tMjAyMi0yMy5hc3B4PjxiPm1vcmU8L2I%2BPC9hPmQCAw9kFgJmDxUDFVNhdHlhc2hvZGhhayBNb3ZlbW
VudJcBQSBzZXNzaW9uIG9uICJTYXR5YXNob2RoYWsgTW92ZW1lbnQiIHdhcyBoZWxkIGluIENvbGxlZ2Ugb24gMjF
zdCBTZXB0ZW1iZXIgMjAyMi4gVGhlIHNlc3Npb24gd2FzIGluYXVndXJhdGVkIGJ5IFNocmkuIE5hbFzYWhlYmpp
IEJvcmFzdGUuIFNlc3Npb24gdy4uLlc8YSBocmVmPWh0dHA6Ly93d3cuY21jc2NvbGxlZ2UuYWMuaW4vbmV3cy80N
C9zYXR5YXNob2RoYWstbW92ZW1lbnQuYXNweD48Yj5tb3JlPC9iPjwvYT5kZAa94prXpierpunkP3j/ojivBLdw&_
_VIEWSTATEGENERATOR=CA0B0334
```

/news.aspx

Details

Strings extracted from ViewState (truncated):

-242440674 _!ItemCount NPh.D. Admission 2022-23 Interview is scheduled on 8th February 2023 at 08:00am Avishkar Competition 2022-23 "Avishkar Competition 2022-23" was held in College on 14th September 2022. A total of 50 student groups participated in this com </span><span class="directors" style="box-sizing: border-box; font-family: Verdana, Arial, Helvetica, sans-serif; color: rgb(0,

Request headers

```
POST /news.aspx?NewsId=43 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 2438
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

__EVENTARGUMENT=1&__EVENTTARGET=1&__VIEWSTATE=/wEPDwUKLTI0MjQ0MDY3NA9kFgJmD2QWAmYPZBYEAgE
PFgIeC18hSXRlbUNvdW50AgEWAgIBD2QWAmYPFQJOUGguRC4gQWRtaXNzaW9uIDIwMjItMjMgSW50ZXJ2aWV3IGlz
IHNjaGVkdWxlZCBvbiA4dGggRmVicnVhcnkgMjAyMyBhdCAwODowMGFtAGQCBg9kFgRmDxYCHwACARYCZg9kFgJmD
xUCHEF2aXNoa2FyIENvbXBldGl0aW9uIDIwMjItMjOoBTxwPgoJIkF2aXNoa2FyIENvbXBldGl0aW9uIDIwMjItMj
MiIHdhcyBoZWxkIGluIENvbGxlZ2Ugb24gMTR0aCBTZXB0ZW1iZXIgMjAyMi4gQSB0b3RhbCBvZiA1MCBzdHVkZW5
0IGdyb3VwcyBwYXJ0aWNpcGF0ZWQgaW4gdGhpcyBjb21wZXRpdGlvbi4gSW5hdWd1cmF0aW9uIG9mIHNhaWQgY29t
cGV0aXRpb24gd2FzIGRvbmUgYnkgPHNwYW4gc3R5bGU9ImNvbG9yOiByZ2IoMCwgMCwgMCk7IGZvbnQtZmFtaWx5O
iBWZXJkYW5hLCBBcmlhbCwgSGVsdmV0aWNhLCBzYW5zLXNlcmlmOyB0ZXh0LWFsaWduOiBqdXN0aWZ5OyI%2BU2hy
aS4gQWR2LiBMYXhtYW4gTGFuZGFnZSAoRGlyZWN0b3IsIE1WUCkgYW5kwqA8L3NwYW4%2BPHNwYW4gY2xhc3M9ImR
pcmVjdG9ycyIgc3R5bGU9ImJveC1zaXppbmc6IGJvcmRlci1ib3g7IGZvbnQtZmFtaWx5OiBWZXJkYW5hLCBBcmlh
bCwgSGVsdmV0aWNhLCBzYW5zLXNlcmlmOyBjb2xvcjogcmdiKDAsIDAsIDApOyB0ZXh0LWFsaWduOiBqdXN0aWZ5O
yI%2BwqA8L3NwYW4%2BPHNwYW4gc3R5bGU9ImNvbG9yOiByZ2IoMCwgMCwgMCk7IGZvbnQtZmFtaWx5OiB2ZXJkYW
5hLCBnZW5ldmEsIHNhbnMtc2VyaWY7IHRleHQtYWxpZ246IGp1c3RpZnk7Ij5TaHJpLiBSYW1lc2ggUGluZ2FsZSA
oRGlyZWN0b3IsIE1WUCkuPC9zcGFuPjwvcD4KPHA%2BCgnCoDwvcD4KPHA%2BCgnCoDwvcD4KZAIBD2QWAmYPFgIf
AAIDFgYCAQ9kFgJmDxUDF1BoLkQuIEFkbWlzc2lvbiAyMDIyLTIzmAFJbnRlcnZpZXdzIGZvciBQaC5ELiBhZG1pc
3Npb25zIHdpbGwgYmUgaGVsZCBvbiA4dGggRmVicnVhcnkgMjAyMyBhdCAwOC4wMCBhLm0uCgoJwqAKCglDYW5kaW
RhdGVzIGFyZSByZXF1aXJlZCB0byBicmluZyBhbG9uZyB3aXRoIHRoZW0gdGhlIGZvbGxvd2luZy4uLlc8YSBocmV
mPWh0dHA6Ly93d3cuY21jc2NvbGxlZ2UuYWMuaW4vbmV3cy80NS9waGQtYWRtaXNzaW9uLTIwMjItMjMuYXNweD48
Yj5tb3JlPC9iPjwvYT5kAgIPZBYCZg8VAxxBdmlzaGthciBDb21wZXRpdGlvbiAyMDIyLTIzlwEiQXZpc2hrYXIgQ
29tcGV0aXRpb24gMjAyMi0yMyIgd2FzIGhlbGQgaW4gQ29sbGVnZSBvbiAxNHRoIFNlcHRlbWJlciAyMDIyLiBBIH
RvdGFsIG9mIDUwIHN0dWRlbnQgZ3JvdXBzIHBhcnRpY2lwYXRlZCBpbiB0aGlzIGNvbXBldGl0aW9uLiBJbmF1Z3V
yYXRpLi4uXjxhIGhyZWY9aHR0cDovL3d3dy5jbWNzY29sbGVnZS5hYy5pbi9uZXdzLzQzL2F2aXNoa2FyLWNvbXBl
dGl0aW9uLTIwMjItMjMuYXNweD48Yj5tb3JlPC9iPjwvYT5kAgMPZBYCZg8VAxVTYXR5YXNob2RoYWsgTW92ZW1lb
nSXAUEgc2Vzc2lvbiBvbiAiU2F0eWFzaG9kaGFrIE1vdmVtZW50IiB3YXMgaGVsZCBpbiBDb2xsZWdlIG9uIDIxc3
QgU2VwdGVtYmVyIDIwMjIuIFRoZSBzZXNzaW9uIHdhcyBpbmF1Z3VyYXRlZCBieSBTaHJpLiBOYW5hc2FoZWJqaSB
Cb3Jhc3RlLiBTZXNzaW9uIHcuLi5XPGEgaHJlZj1odHRwOi8vd3d3LmNtY3Njb2xsZWdlLmFjLmluL25ld3MvNDQv
c2F0eWFzaG9kaGFrLW1vdmVtZW50LmFzcHg%2BPGI%2BbW9yZTwvYj48L2E%2BZGQPWlKA4nz/pKOnhTbBLC4e2gQ
jqQ==&__VIEWSTATEGENERATOR=CA8C29DA
```

/news/43/avishkar-competition-2022-23.aspx

Details

Strings extracted from ViewState (truncated):

-242440674 _!ItemCount NPh.D. Admission 2022-23 Interview is scheduled on 8th February 2023 at 08:00am Avishkar Competition 2022-23 "Avishkar Competition 2022-23" was held in College on 14th September 2022. A total of 50 student groups participated in this com </span><span class="directors" style="box-sizing: border-box; font-family: Verdana, Arial, Helvetica, sans-serif; color: rgb(0,

Request headers

```
GET /news/43/avishkar-competition-2022-23.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/news/44/satyashodhak-movement.aspx

Details

Strings extracted from ViewState (truncated):

-242440674 _!ItemCount NPh.D. Admission 2022-23 Interview is scheduled on 8th February 2023 at 08:00am Satyashodhak Movement A session on "Satyashodhak Movement" was held in College on 21st September 2022. The session was inaugurated by Shri. Nanasahebj Ph.D. Admission 2022-23

Request headers

```
GET /news/44/satyashodhak-movement.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/news/45/phd-admission-2022-23.aspx

Details

Strings extracted from ViewState (truncated):

-242440674 _!ItemCount NPh.D. Admission 2022-23 Interview is scheduled on 8th February 2023 at 08:00am Ph.D. Admission 2022-23 <div> Interviews for Ph.D. admissions will be held on 8th February 2023 at 08.00 a.m.</div>

Request headers

```
GET /news/45/phd-admission-2022-23.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/pageinfo.aspx

Details

Strings extracted from ViewState (truncated):

1368401346 _!ItemCount NPh.D. Admission 2022-23 Interview is scheduled on 8th February 2023 at 08:00am 6http://www.cmcscollege.ac.in/img/slider-auditorium.jpgd class 0col-lg-12 col-md-12 col-sm-12 col-xs-12 pad-LR-0

Request headers

```
POST /pageinfo.aspx?PageId=37 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 3088
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

__EVENTARGUMENT=1&__EVENTTARGET=1&__EVENTVALIDATION=/wEWAgLO8M/yDgKF4t3bDAMCuOlPWsewwBsT5
l/p0jGurk3K&__VIEWSTATE=/wEPDwUKMTM2ODQwMTM0Ng9kFgJmD2QWAmYPZBYEAgEPFgIeC18hSXRlbUNvdW50A
gEWAgIBD2QWAmYPFQJOUGguRC4gQWRtaXNzaW9uIDIwMjItMjMgSW50ZXJ2aWV3IGlzIHNjaGVkdWxlZCBvbiA4dG
ggRmVicnVhcnkgMjAyMyBhdCAwODowMGFtAGQCBg9kFgYCAQ8WAh8AAgEWAmYPZBYCZg8VATZodHRwOi8vd3d3LmN
tY3Njb2xsZWdlLmFjLmluL2ltZy9zbGlkZXItYXVkaXRvcml1bS5qcGdkAgUPFgIeBWNsYXNzBTBjb2wtbGctMTIg
Y29sLW1kLTEyIGNvbC1zbS0xMiBjb2wteHMtMTIgcGFkLUxSLTAWAmYPZBYCAgEPFgIeCWlubmVyaHRtbAWoBzxka
XYgY2xhc3M9InRpdGxlIj4KCTxzdHJvbmc%2BSW5mcmFzdHJ1Y3R1cmU6IEF1ZGl0b3JpdW08L3N0cm9uZz48L2Rp
dj4KPHRhYmxlIGJvcmRlcj0iMSIgY2VsbHBhZGRpbmc9IjAiIGNlbGxzcGFjaW5nPSIwIj4KCTx0Ym9keT4KCQk8d
HI%2BCgkJCTx0ZD4KCQkJCTxwIGFsaWduPSJjZW50ZXIiPgoJCQkJCTxzdHJvbmc%2BU3IuIE5vPC9zdHJvbmc%2B
PC9wPgoJCQk8L3RkPgoJCQk8dGQ%2BCgkJCQk8cCBhbGlnbj0iY2VudGVyIj4KCQkJCQk8c3Ryb25nPkluZnJhc3R
ydWN0dXJlPC9zdHJvbmc%2BPC9wPgoJCQk8L3RkPgoJCQk8dGQ%2BCgkJCQk8cCBhbGlnbj0iY2VudGVyIj4KCQkJ
CQk8c3Ryb25nPkRpbWVuc2lvbjwvc3Ryb25nPjwvcD4KCQkJPC90ZD4KCQkJPHRkPgoJCQkJPHAgYWxpZ249ImNlb
nRlciI%2BCgkJCQkJPHN0cm9uZz5BcmVhKFNxLk0uKTwvc3Ryb25nPjwvcD4KCQkJPC90ZD4KCQk8L3RyPgoJCTx0
cj4KCQkJPHRkPgoJCQkJPHAgYWxpZ249ImNlbnRlciI%2BCgkJCQkJMTwvcD4KCQkJPC90ZD4KCQkJPHRkPgoJCQk
JQXVkaXRvcml1bTwvdGQ%2BCgkJCTx0ZD4KCQkJCTExLjM1WDE5LjI1PC90ZD4KCQkJPHRkPgoJCQkJMjE4LjQ4PC
90ZD4KCQk8L3RyPgoJCTx0cj4KCQkJPHRkPgoJCQkJPHAgYWxpZ249ImNlbnRlciI%2BCgkJCQkJMjwvcD4KCQkJP
C90ZD4KCQkJPHRkPgoJCQkJU291bmQgU3lzdGVtIFJvb208L3RkPgoJCQk8dGQ%2BCgkJCQkzLjY1WDMuODU8L3Rk
PgoJCQk8dGQ%2BCgkJCQkxNC4wNTwvdGQ%2BCgkJPC90cj4KCQk8dHI%2BCgkJCTx0ZD4KCQkJCTxwIGFsaWduPSJ
jZW50ZXIiPgoJCQkJCTM8L3A%2BCgkJCTwvdGQ%2BCgkJCTx0ZD4KCQkJCUF1ZGl0b3JpdW0gU3RvcmUgUm9vbTwv
dGQ%2BCgkJCTx0ZD4KCQkJCTEuNTBYMy44MDwvdGQ%2BCgkJCTx0ZD4KCQkJCTUuNzwvdGQ%2BCgkJPC90cj4KCTw
vdGJvZHk%2BCjwvdGFibGU%2BCjxwPgoJwqA8L3A%2BCmQCBw8PFgIeB1Zpc2libGVoZBYCZg8WAh8AAgMWBgIBD2
QWAmYPFQMXUGguRC4gQWRtaXNzaW9uIDIwMjItMjOYAUludGVydmlld3MgZm9yIFBoLkQuIGFkbWlzc2lvbnMgd2l
sbCBiZSBoZWxkIG9uIDh0aCBGZWJydWFyeSAyMDIzIGF0IDA4LjAwIGEubS4KCgnCoAoKCUNhbmRpZGF0ZXMgYXJl
IHJlcXVpcmVkIHRvIGJyaW5nIGFsb25nIHdpdGggdGhlbSB0aGUgZm9sbG93aW5nLi4uVzxhIGhyZWY9aHR0cDovL
3d3dy5jbWNzY29sbGVnZS5hYy5pbi9uZXdzLzQ1L3BoZC1hZG1pc3Npb24tMjAyMi0yMy5hc3B4PjxiPm1vcmU8L2
I%2BPC9hPmQCAg9kFgJmDxUDHEF2aXNoa2FyIENvbXBldGl0aW9uIDIwMjItMjOXASJBdmlzaGthciBDb21wZXRpd
GlvbiAyMDIyLTIzIiB3YXMgaGVsZCBpbiBDb2xsZWdlIG9uIDE0dGggU2VwdGVtYmVyIDIwMjIuIEEgdG90YWwgb2
YgNTAgc3R1ZGVudCBncm91cHMgcGFydGljaXBhdGVkIGluIHRoaXMgY29tcGV0aXRpb24uIEluYXVndXJhdGkuLi5
ePGEgaHJlZj1odHRwOi8vd3d3LmNtY3Njb2xsZWdlLmFjLmluL25ld3MvNDMvYXZpc2hrYXItY29tcGV0aXRpb24t
MjAyMi0yMy5hc3B4PjxiPm1vcmU8L2I%2BPC9hPmQCAw9kFgJmDxUDFVNhdHlhc2hvZGhhayBNb3ZlbWVudJcBQSB
zZXNzaW9uIG9uICJTYXR5YXNob2RoYWsgTW92ZW1lbnQiIHdhcyBoZWxkIGluIENvbGxlZ2Ugb24gMjFzdCBTZXB0
ZW1iZXIgMjAyMi4gVGhlIHNlc3Npb24gd2FzIGluYXVndXJhdGVkIGJ5IFNocmkuIE5hbmFzYWhlYmppIEJvcmFzd
GUuIFNlc3Npb24gdy4uLlc8YSBocmVmPWh0dHA6Ly93d3cuY21jc2NvbGxlZ2UuYWMuaW4vbmV3cy80NC9zYXR5YX
Nob2RoYWstbW92ZW1lbnQuYXNweD48Yj5tb3JlPC9iPjwvYT5kZGwnd2JGCRbSkuAs1wVghtSMmQvR&__VIEWSTAT
EGENERATOR=429198DF&ctl00%24ContentPlaceHolder1%24hdnPageId=37
```

❗ Vulnerable Javascript library

Severity	**Medium**
Reported by module	/Scripts/PerFile/Javascript_Libraries_Audit.script

Description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

Recommendation

Upgrade to the latest version.

Affected items

/js/jquery.js

Verified vulnerability

Details

Detected Javascript library **jquery** version **1.11.0**.
The version was detected from **syntax fingerprint, syntax fingerprint**.

References:

- https://github.com/jquery/jquery/issues/2432
- http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

Request headers

```
GET /js/jquery.js HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/js/jquery.min.js

Verified vulnerability

Details

Detected Javascript library **jquery** version **1.11.1**.
The version was detected from **syntax fingerprint, syntax fingerprint**.

References:

- https://github.com/jquery/jquery/issues/2432
- http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/

Request headers

```
GET /js/jquery.min.js HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

ASP.NET version disclosure

Severity	**Low**
Reported by module	/Scripts/PerServer/ASP_NET_Error_Message.script

Description

The HTTP responses returned by this web application include anheader named **X-AspNet-Version**. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled.

Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Apply the following changes to the web.config file to prevent ASP.NET version disclosure:

```
<System.Web>
 <httpRuntime enableVersionHeader="false" />
</System.Web>
```

References

HttpRuntimeSection.EnableVersionHeader Property (https://docs.microsoft.com/en-us/dotnet/api/system.web.configuration.httpruntimesection.enableversionheader?redirectedfrom=MSDN&view=netframework-4.8#System_Web_Configuration_HttpRuntimeSection_EnableVersionHeader)

Affected items

Web Server

Details

Version information found:

```
2.0.50727
```

Request headers

```
GET /|~.aspx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	/Scripts/PerServer/Clickjacking_X_Frame_Options.script

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)
Clickjacking (https://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive (https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server

Details

Request headers

```
GET / HTTP/1.1
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

ⓘ Cookie(s) without Secure flag set

Severity	**Low**
Reported by module	/RPA/Cookie_Without_Secure.js

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

Web Server
Verified vulnerability
Details
Set-Cookie: ASP.NET_SessionId=hwouhr55pwrleknwaygoox45; path=/; HttpOnly
Request headers

```
GET / HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Session token in URL

Severity	**Low**
Reported by module	/RPA/Session_Token_In_Url.js

Description

This application contains a session token in the query parameters. A session token is sensitive information and should not be stored in the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

Recommendation

The session should be maintained using cookies (or hidden input fields).

Affected items

/news.aspx
Details
Request headers

```
POST /news.aspx?NewsId=43 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 2438
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive

__EVENTARGUMENT=1&__EVENTTARGET=1&__VIEWSTATE=/wEPDwUKLTI0MjQ0MDY3NA9kFgJmD2QWAmYPZBYEAgE
PFgIeC18hSXRlbUNvdW50AgEWAgIBD2QWAmYPFQJOUGguRC4gQWRtaXNzaW9uIDIwMjItMjMgSW50ZXJ2aWV3IGlz
IHNjaGVkdWxlZCBvbiA4dGggRmVicnVhcnkgMjAyMyBhdCAwODowMGFtAGQCBg9kFgRmDxYCHwACARYCZg9kFgJmD
xUCHEF2aXNoa2FyIENvbXBldGl0aW9uIDIwMjItMjOoBTxwPgoJIkF2aXNoa2FyIENvbXBldGl0aW9uIDIwMjItMj
MiIHdhcyBoZWxkIGluIENvbGxlZ2Ugb24gMTR0aCBTZXB0ZW1iZXIgMjAyMi4gQSB0b3RhbCBvZiA1MCBzdHVkZW5
0IGdyb3VwcyBwYXJ0aWNpcGF0ZWQgaW4gdGhpcyBjb21wZXRpdGlvbi4gSW5hdWd1cmF0aW9uIG9mIHNhaWQgY29t
cGV0aXRpb24gd2FzIGRvbmUgYnkgPHNwYW4gc3R5bGU9ImNvbG9yOiByZ2IoMCwgMCwgMCk7IGZvbnQtZmFtaWx5O
iBWZXJkYW5hLCBBcmlhbCwgSGVsdmV0aWNhLCBzYW5zLXNlcmlmOyB0ZXh0LWFsaWduOiBqdXN0aWZ5OyI%2BU2hy
aS4gQWR2LiBMYXhtYW4gTGFuZGFnZSAoRGlyZWN0b3IsIE1WUCkgYW5kwqA8L3NwYW4%2BPHNwYW4gY2xhc3M9ImR
pcmVjdG9ycyIgc3R5bGU9ImJveC1zaXppbmc6IGJvcmRlci1ib3g7IGZvbnQtZmFtaWx5OiBWZXJkYW5hLCBBcmlh
bCwgSGVsdmV0aWNhLCBzYW5zLXNlcmlmOyBjb2xvcjogcmdiKDAsIDAsIDApOyB0ZXh0LWFsaWduOiBqdXN0aWZ5O
yI%2BwqA8L3NwYW4%2BPHNwYW4gc3R5bGU9ImNvbG9yOiByZ2IoMCwgMCwgMCk7IGZvbnQtZmFtaWx5OiB2ZXJkYW
5hLCBnZW5ldmEsIHNhbnMtc2VyaWY7IHRleHQtYWxpZ246IGp1c3RpZnk7Ij5TaHJpLiBSYW1lc2ggUGluZ2FsZSA
oRGlyZWN0b3IsIE1WUCkuPC9zcGFuPjwvcD4KPHA%2BCgnCoDwvcD4KPHA%2BCgnCoDwvcD4KZAIBD2QWAmYPFgIf
AAIDFgYCAQ9kFgJmDxUDF1BoLkQuIEFkbWlzc2lvbiAyMDIyLTIzmAFJbnRlcnZpZXdzIGZvciBQaC5ELiBhZG1pc
3Npb25zIHdpbGwgYmUgaGVsZCBvbiA4dGggRmVicnVhcnkgMjAyMyBhdCAwOC4wMCBhLm0uCgoJwqAKCglDYW5kaW
RhdGVzIGFyZSByZXF1aXJlZCB0byBicmluZyBhbG9uZyB3aXRoIHRoZW0gdGhlIGZvbGxvd2luZy4uLlc8YSBocmV
mPWh0dHA6Ly93d3cuY21jc2NvbGxlZ2UuYWMuaW4vbmV3cy80NS9waGQtYWRtaXNzaW9uLTIwMjItMjMuYXNweD48
Yj5tb3JlPC9iPjwvYT5kAgIPZBYCZg8VAxxBdmlzaGthciBDb21wZXRpdGlvbiAyMDIyLTIzlwEiQXZpc2hrYXIgQ
29tcGV0aXRpb24gMjAyMi0yMyIgd2FzIGhlbGQgaW4gQ29sbGVnZSBvbiAxNHRoIFNlcHRlbWJlciAyMDIyLiBBIH
RvdGFsIG9mIDUwIHN0dWRlbnQgZ3JvdXBzIHBhcnRpY2lwYXRlZCBpbiB0aGlzIGNvbXBldGl0aW9uLiBJbmF1Z3V
yYXRpLi4uXjxhIGhyZWY9aHR0cDovL3d3dy5jbWNzY29sbGVnZS5hYy5pbi9uZXdzLzQzL2F2aXNoa2FyLWNvbXBl
dGl0aW9uLTIwMjItMjMuYXNweD48Yj5tb3JlPC9iPjwvYT5kAgMPZBYCZg8VAxVTYXR5YXNob2RoYWsgTW92ZW1lb
nSXAUEgc2Vzc2lvbiBvbiAiU2F0eWFzaG9kaGFrIE1vdmVtZW50IiB3YXMgaGVsZCBpbiBDb2xsZWdlIG9uIDIxc3
QgU2VwdGVtYmVyIDIwMjIuIFRoZSBzZXNzaW9uIHdhcyBpbmF1Z3VyYXRlZCBieSBTaHJpLiBOYW5hc2FoZWJqaSB
Cb3Jhc3RlLiBTZXNzaW9uIHcuLi5XPGEgaHJlZj1odHRwOi8vd3d3LmNtY3Njb2xsZWdlLmFjLmluL25ld3MvNDQv
c2F0eWFzaG9kaGFrLW1vdmVtZW50LmFzcHg%2BPGI%2BbW9yZTwvYj48L2E%2BZGQPWlKA4nz/pKOnhTbBLC4e2gQ
jqQ==&__VIEWSTATEGENERATOR=CA8C29DA
```

Stack Trace Disclosure (ASP.NET)

Severity	**Low**
Reported by module	/httpdata/text_search.js

Description

A stack trace was identified on this page. The web application has generated an error message that includes sensitive information about its environment, users, or associated data.

The stack trace can disclose potentially sensitive information such as: physical file paths of relevant files, source code fragments, version information of various packages, database information, error messages, ...

It's recommended to handle exceptions internally and do not display errors containing potentially sensitive information to a user.

Impact

The stack trace may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

To prevent the information disclosure you can implement custom error pages by applying the following changes to your **web.config** file.

```
<System.Web>
     <customErrors mode="On" defaultRedirect="~/error/GeneralError.aspx">
          <error statusCode="403" redirect="~/error/Forbidden.aspx" />
          <error statusCode="404" redirect="~/error/PageNotFound.aspx" />
          <error statusCode="500" redirect="~/error/InternalError.aspx" />
     </customErrors>
</System.Web>
```

Affected items

Web Server

Details

Request headers

```
GET /?search=<script>alert(1)</script> HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/|~.aspx

Details

Request headers

```
GET /|~.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Unencrypted connection

Severity	**Low**
Reported by module	/RPA/no_https.js

Description

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

Impact

Possible information disclosure.

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

Affected items

Web Server
Verified vulnerability
Details
Request headers

```
GET / HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Content Security Policy (CSP) not implemented

Severity	**Informational**
Reported by module	/httpdata/CSP_not_implemented.js

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.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
[Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Request headers

```
GET / HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

ⓘ Email address found

Severity	**Informational**
Reported by module	/Scripts/PerFile/Text_Search_File.script

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)](https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

/Grievances-Redressal-Cell.aspx
Details

Pattern found:

```
bankar.prashant1887@gmail.com
```

Request headers

```
GET /Grievances-Redressal-Cell.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/Health-center.aspx

Details

Pattern found:

```
77.archana@gmail.com
```

Request headers

```
GET /Health-center.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/Linkages.aspx

Details

Pattern found:

```
mail@webvisionlabs.com
softhealtech@gmail.com
pvntransformer@rediffmail.com
```

Request headers

```
GET /Linkages.aspx HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Error page web server version disclosure

Severity	**Informational**

Reported by module	/Scripts/PerServer/Error_Page_Path_Disclosure.script

Description

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

Custom Error Responses (Apache HTTP Server) (https://httpd.apache.org/docs/current/custom-error.html)
server_tokens (Nginx) (http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens)
Remove Unwanted HTTP Response Headers (Microsoft IIS)
(https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/)

Affected items

Web Server

Details

Pattern found:

```
Microsoft .NET Framework Version:2.0.50727.9055; ASP.NET Version:2.0.50727.9051
```

Request headers

```
GET /Ev6FQbpDof.aspx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

ⓘ Microsoft IIS version disclosure

Severity	**Informational**
Reported by module	/Scripts/PerServer/ASP_NET_Error_Message.script

Description

The HTTP responses returned by this web application include a header named **Server**. The value of this header includes the version of Microsoft IIS server.

Impact

The HTTP header may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult web references for more information.

References

Remove Unwanted HTTP Response Headers (https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/)

Affected items

Web Server

Details

Version information found:

```
Microsoft-IIS/10.0
```

Request headers

```
GET /|~.aspx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Possible username or password disclosure

Severity	**Informational**
Reported by module	/Scripts/PerFile/Text_Search_File.script

Description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/font-awesome-4.3.0/font-awesome-4.3.0/css/font-awesome.css

Details

Pattern found:

```
pass:before
```

Request headers

```
GET /font-awesome-4.3.0/font-awesome-4.3.0/css/font-awesome.css HTTP/1.1
Referer: http://www.cmcscollege.ac.in/
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Web Application Firewall detected

Severity	**Informational**
Reported by module	/Scripts/PerServer/WAF_Detection.script

Description

This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

Impact

You may receive incorrect/incomplete results when scanning a server protected by an IPS/IDS/WAF. Also, if the WAF detects a number of attacks coming from the scanner, the IP address can be blocked after a few attempts.

Recommendation

If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

Affected items

Web Server

Details

Detected ASP.NET RequestValidation from the response body.

Request headers

```
GET /?search=<script>alert(1)</script> HTTP/1.1
Cookie: ASP.NET_SessionId=zrbysnyhu5bsxl45t3e45i55
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: www.cmcscollege.ac.in
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Scanned items (coverage report)

http://www.cmcscollege.ac.in/
http://www.cmcscollege.ac.in/Auditorium.aspx
http://www.cmcscollege.ac.in/Default.aspx
http://www.cmcscollege.ac.in/Ev6FQbpDof.aspx
http://www.cmcscollege.ac.in/Grievances-Redressal-Cell.aspx
http://www.cmcscollege.ac.in/Health-center.aspx
http://www.cmcscollege.ac.in/Linkages.aspx
http://www.cmcscollege.ac.in/ScriptResource.axd
http://www.cmcscollege.ac.in/WebResource.axd
http://www.cmcscollege.ac.in/alumini.aspx
http://www.cmcscollege.ac.in/font-awesome-4.3.0/font-awesome-4.3.0/css/font-awesome.css
http://www.cmcscollege.ac.in/js/jquery.js
http://www.cmcscollege.ac.in/js/jquery.min.js
http://www.cmcscollege.ac.in/news.aspx
http://www.cmcscollege.ac.in/news/43/avishkar-competition-2022-23.aspx
http://www.cmcscollege.ac.in/news/44/satyashodhak-movement.aspx
http://www.cmcscollege.ac.in/news/45/phd-admission-2022-23.aspx
http://www.cmcscollege.ac.in/pageinfo.aspx
http://www.cmcscollege.ac.in/teacherprofile.aspx
http://www.cmcscollege.ac.in/|~.aspx