

Developer Report

Acunetix Security Audit

17 July 2019

Scan of tptuat.aponline.gov.in

Scan details

Scan information		
Start time	16/07/2019, 21:58:01	
Start url	https://tptuat.aponline.gov.in/pollutioncb/	
Host	tptuat.aponline.gov.in	
Scan time	20 minutes, 18 seconds	
Profile	Full Scan	
Responsive	True	
Server OS	Windows	
Server technologies	ASP	

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	25
1 High	0
Medium	13
① Low	6
1 Informational	6

Alerts summary

• 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	1
/pollutioncb/AppointmentMS.aspx	2
/pollutioncb/feedback.aspx	1
/pollutioncb/nationaa_ambient_air_quality_m	onitoring.aspx 2

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: Lov Privileges Required: Nouser Interaction: None Scope: Unchanged Confidentiality Impact: Integrity Impact: None Availability Impact: Nore	v one High
CWE	WE CWE-200	
Affected items		Variation
Web Server		1
/pollutioncb/a_external_advisory_committe_New.aspx		1
/pollutioncb/a_real_time_noise_monitoring_stations.aspx		1
/pollutioncb/content-management-cfe.aspx		1
/pollutioncb/content-management-cfo.aspx		1
/pollutioncb/continuous-ambient-air-quality-monitoring-stations-caaqms.aspx		1
/pollutioncb/feedback.aspx		1

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	

① Clickjacking: X-Frame-Options header missing

(Classification
---	----------------

CWE CWE	et Distribution: Not_defined -693
Acces Acces Auther Confir Integr Availa CVSS2 Explo Reme Repo Availa Collat Confir Integr	Score: 6.8 ss Vector: Network_accessible ss Complexity: Medium entication: None dentiality Impact: Partial rity Impact: Partial ability Impact: Partial bitability: Not_defined ediation Level: Not_defined art Confidence: Not_defined ability Requirement: Not_defined teral Damage Potential: Not_defined dentiality Requirement: Not_defined rity Requirement: Not_defined

Possible sensitive directories

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	
Web Server	1	

① Stack Trace Disclosure (ASP.NET)

Classification

CWE Affected items /pollutioncb/AppointmentMS.aspx	Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined CWE-209 Variation 1	
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	

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
/pollutioncb/a_ProcedureforOnlineConnectivity.htm		1
/pollutioncb/bio-medical-waste-management.html		1
/pollutioncb/contact-us.html		1
/pollutioncb/hazardous-waste-management.html		1

1 Possible internal IP address disclosure

\sim		4.5
('	lacciti	cation
\sim	ıassııı	caucii

/pollutioncb/a_external_advisory_committe_New.aspx		1
CWE Affected items	CWE-200	Variation
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: No User Interaction: None Scope: Unchanged Confidentiality Impact: Integrity Impact: None Availability Impact: None	one High
CVSS2	Base Score: 5.0 Access Vector: Network Access Complexity: Low Authentication: None Confidentiality Impact: Integrity Impact: None Availability Impact: None Exploitability: Not_defin Remediation Level: Not Report Confidence: Not Availability Requirement Collateral Damage Pote Confidentiality Requirement: Integrity Requirement: Target Distribution: Not	Partial ne ned t_defined t_defined nt: Not_defined ential: Not_defined ment: Not_defined Mot_defined

① Subresource Integrity (SRI) 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
<u>/pollutioncb/</u>	1

Application error message

Severity	Medium
Reported by module	/Scripts/PerScheme/Error_Message.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 (http://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 "" (empty)

Pattern found:

ASP.NET is configured to show verbose error messages

Request headers

GET /pollutioncb/.aspx HTTP/1.1

Referer: https://tptuat.aponline.gov.in/pollutioncb/

Connection: keep-alive

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

/pollutioncb/AppointmentMS.aspx

Details

URL encoded POST input txtnameofperson was set to ZIZIZzRFb0s=

Pattern found:

ASP.NET is configured to show verbose error messages

Request headers

POST /pollutioncb/AppointmentMS.aspx HTTP/1.1 Content-Type: application/x-www-form-urlencoded

Connection: keep-alive

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate

Content-Length: 1731

Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

EVENTVALIDATION=/wEdABp/vaanXNMTbZclx2Luly/1JGAFvP3BWIYdnqm0xGD33hffPEYN0Gr%2B8o/R36bDn DoJ8f01hK1tIAud3QCqieFtV6ItGWtk/kC83AupZud3nLway05GmvzqD/esPsVzqRcTV2Yd7dvrU47ouI8JLzlHEx IA608hWwIWORKCudq9qVPC55siuOfYvXn2zJs0YU6NTFqNzNYcj3CTUD0nnR8zauZDiGNqsUq2VT0ADu3BqeHcEqJ d9wUWvSVgjtUL9qJCnLEzADTFxrML8S8XzLr8HNLcCfRk48iVzk64o4qWLFvrQXKHGRPJi1DZ4aaHXnaaQRNj27JB RdBAmQI9QHVddap7eM06KOJY0n9H1tNS4nJnJn/4UdbTlCbihLSSSuTYEojqdGq3Mu8Lu0xZ8QsdwsQHZSqtak0Gc kVf30r3B3ZawmrS7mAaCEircaMTjVasEpMGhMrWor0WDE0xpvK4%2BQID2tpjfSbwT6WuVmLKZjsvgabDL71Ho8Un Fk4qIY3/H1A8JePMN6iGHckUTZUZPOaW1pQztoQA36D1w/%2BbXUIi7FK5z70XmmUAb8SHCvzhG01Hbb0gf0tkeBt 9aAoE& VIEWSTATE=/wEPDwUIMzY4MDY5MzUPZBYCAgMPZBYCAgMPEA8WBh4NRGF0YVRleHRGaWVsZAUUZGlzdHJ pY3RfZGVzY3JpcHRpb24eDkRhdGFWYWx1ZUZpZWxkBQtkaXN0cmljdF9pZB4LXyFEYXRhQm91bmRnZBAVDgZTZWxl Y3QeU3Jpa2FrdWxhbSAgICAgICAgICAgICAgICAgICAgICAgH1ZpemlhbmFnYXJhbSAgICAgICAgICAgICAgIB5Wa XNha2hhcGF0bmFtICAgICAgICAgICAgICAgICAeRWFzdCBHb2RhdmFyaSAgICAgICAgICAgICAgICAgHldlc3QgR2 9kYXZhcmkgICAgICAgICAgICAgICAgIB5LcmlzaG5hICAgICAgICAgICAgICAgICAgICAgICAgICAGICACAGICAGICAGICAGICAGICAGICAGICA gICAgICAgICAgICAgICAgICAgHlByYWthc2FtICAgICAgICAgICAgICAgICAgICAgIB5TcmkgUG90dGkgU3JpcmFt dWx1IE5lbGxvcmUgICAeQ2hpdHRvb3IgICAgICAgICAgICAgICAgICAgICAgHlkuUy5SLiAgICAgICAgICAgICAGI CAgICAgICAgIB5BbmFudGhhcHVyYW111CAgICAgICAgICAgICAGICAeS3Vybm9vbCAgICAgICAgICAgICAgICAGICAGIC AgICAgFQ4CMDACMDECMDICMDMCMDQCMDUCMDYCMDcCMDgCMDkCMTACMTECMTICMTMUKwMOZ2dnZ2dnZ2dnZ2dnZ2d kZGQht64Wr5uU8XjDUREjqNuvndayjLI/63ZAMX9pO5OnFw==& VIEWSTATEGENERATOR=0A3DDF53&btnSubmit =Submit&ddldist=00&rdoappoint=01&txtdateofvisite=http://www.vulnweb.com&txtdesignation=1& txtemail=sample%40email.tst&txtmobilenumber=987-65-

4329&txtnameofperson=Z1Z1ZzRFb0s=&txtnameofunit=CpjJwWHV&txtpurposeofviste=555

/pollutioncb/AppointmentMS.aspx

Details

URL encoded POST input txtnameofunit was set to aEF4OHR3SXk=

Pattern found:

ASP.NET is configured to show verbose error messages

POST /pollutioncb/AppointmentMS.aspx HTTP/1.1 Content-Type: application/x-www-form-urlencoded

Connection: keep-alive

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate

Content-Length: 1731

Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

EVENTVALIDATION=/wEdABp/vaanXNMTbZclx2Luly/1JGAFvP3BWIYdnqm0xGD33hffPEYN0Gr%2B8o/R36bDn DoJ8f01hK1tIAud3QCqieFtV6ItGWtk/kC83AupZud3nLway05GmvzqD/esPsVzqRcTV2Yd7dvrU47ouI8JLz1HEx IA608hWwIWORKCudq9qVPC55siuOfYvXn2zJs0YU6NTFqNzNYcj3CTUD0nnR8zauZDiGNqsUq2VT0ADu3BqeHcEqJ d9wUWvSVgjtUL9qJCnLEzADTFxrML8S8XzLr8HNLcCfRk48iVzk64o4qWLFvrQXKHGRPJi1DZ4aaHXnaaQRNj27JB RdBAmQI9QHVddap7eM06KOJY0n9H1tNS4nJnJn/4UdbTlCbihLSSSuTYEojgdGq3Mu8Lu0xZ8QsdwsQHZSgtak0Gc kVf30r3B3ZawmrS7mAaCEircaMTjVasEpMGhMrWor0WDE0xpvK4%2BQID2tpjfSbwT6WuVmLKZjsvgabDL71Ho8Un Fk4qIY3/H1A8JePMN6iGHckUTZUZPOaW1pQztoQA36D1w/%2BbXUIi7FK5z70XmmUAb8SHCvzhG01Hbb0gf0tkeBt 9aAoE& VIEWSTATE=/wEPDwUIMzY4MDY5MzUPZBYCAqMPZBYCAqMPEA8WBh4NRGF0YVRleHRGaWVsZAUUZGlzdHJ pY3RfZGVzY3JpcHRpb24eDkRhdGFWYWx1ZUZpZWxkBQtkaXN0cmljdF9pZB4LXyFEYXRhQm91bmRnZBAVDgZTZWxl Y3QeU3Jpa2FrdWxhbSAgICAgICAgICAgICAgICAgICAgHlZpemlhbmFnYXJhbSAgICAgICAgICAgICAgIB5Wa XNha2hhcGF0bmFtICAgICAgICAgICAgICAgICAeRWFzdCBHb2RhdmFyaSAgICAgICAgICAgICAgICAgHldlc3QgR2 9kYXZhcmkgICAgICAgICAgICAgICAgIB5LcmlzaG5hICAgICAgICAgICAgICAgICAgICAgICAeR3VudHVyICAgICA gICAgICAgICAgICAgICAgICAgHlByYWthc2FtICAgICAgICAgICAgICAgICAgICAgIB5TcmkgUG90dGkgU3JpcmFt dWx1IE5lbGxvcmUgICAeQ2hpdHRvb3IgICAgICAgICAgICAgICAgICAgICAgICAgHlkuUy5SLiAgICAgICAgICAgICAgI CAqICAqICAqIB5BbmFudGhhcHVyYW111CAqICAqICAqICAqICAqICAeS3Vybm9vbCAqICAqICAqICAqICAqICAqICAqIC AgICAgFQ4CMDACMDECMDICMDMCMDQCMDUCMDYCMDcCMDgCMDkCMTACMTECMTICMTMUKwMOZ2dnZ2dnZ2dnZ2dnZ2d kZGQht64Wr5uU8XjDUREjqNuvndayjLI/63ZAMX9pO5OnFw==& VIEWSTATEGENERATOR=0A3DDF53&btnSubmit =Submit&ddldist=00&rdoappoint=01&txtdateofvisite=http://www.vulnweb.com&txtdesignation=1& txtemail=sample%40email.tst&txtmobilenumber=987-65-

/pollutioncb/feedback.aspx

Details

URL encoded POST input txtname was set to eEE3R01Idm4=

Pattern found:

ASP.NET is configured to show verbose error messages

Request headers

POST /pollutioncb/feedback.aspx HTTP/1.1

Content-Type: application/x-www-form-urlencoded

Connection: keep-alive

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate

Content-Length: 694

Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

 $ImageButton1=1\&_EVENTVALIDATION=/wEdAas7jX9YonL7ZZ6cx9DuyLsOVCDn2pfngd5PS19R1fd0WMjkomTeSEWFH1kGCQje%2BaBnjdbt1ZLOCXGRPBQfNNIqUpniTDrt%2BjARd%2BhUExs4c9gSiOB0arcy7wu7TFnxCx3CxAd1kC1qTQZyRV/fSvcHLd9Mi3j84XpObGQKq4C%2BFs5XhHXFJzWEz/a3lvNJ4KXpkAKvH1FmeWUpJ6tT4i4qPOaW1pQztoQA36D1w/%2BbXR2e1AknqONs0occKNnOwBbt0KC0n755T0yxNBJpjPSK&__VIEWSTATE=/wEPDwUKLTI3OTQ3NzE0N2QYAQUeX19Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgEFDEltYWdlQnV0dG9uMdew1VSfqJiGWM/vQJwf0lxSwPljGz6ttDACVXA6yvgs&__VIEWSTATEGENERATOR=938AE22F&btnSubmit=Submit&txtaddress=3137%20Laguna%20Street&txtdist=1&txtemail=sample%40email.tst&txtfeedbacksuggition=555&txtimgcode=94102&txtmobilenumber=987-65-4329&txtname=eEE3R01Idm4=&txtstate=NY$

/pollutioncb/nationaa_ambient_air_quality_monitoring.aspx

Details

URL encoded POST input ddlDistricts 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 /pollutioncb/nationaa ambient air quality monitoring.aspx HTTP/1.1

Content-Type: application/x-www-form-urlencoded
Referer: https://tptuat.aponline.gov.in/pollutioncb/

Connection: keep-alive

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate

Content-Length: 5544

Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

EVENTARGUMENT=1& EVENTTARGET=1& EVENTVALIDATION=/wEdABEr5oyvUatJpi5ZCqLhk/JmSfCvlfoVl L48NcRF2wf9Vsj7NjLk8E6yomFtP41os9MN4dWy6i45xDdsiJrG2UcdsqeiyN3hqi5atA1mQ%2ByHpjqhHqp60UD3 Qie30xeyGAzi2GjZW84wacFClnLsuZgpRRu047jLP1I5Qvs%2BZpfv9s50CEGQsQdZ6hoeA6M4Tbl0uWjViXg//oK P/ZA4tTFPDqlvECqA%2Bz00bCqquHMzDGCJedmBD1SP1RChwQbdMkORBBqBfUvlUnHqajrJLqh0EtCNEQYsonxWI2 tv/9FTNHa54/aXozq3BrzdY51OG4uudg%2BoI0FBgv5kfHepmIrudNuzUDROkL2sq6dXDTi6WVc7WBe6C60EB93gm c2KThRAKG2OuGNL9J5qQWsuKO7e& LASTFOCUS=1& VIEWSTATE=/wEPDwULLTE0NTIwNjExNzAPZBYCAqMPZBY IAgMPEA8WBh4NRGF0YVRleHRGaWVsZAUIRGlzdHJpY3QeDkRhdGFWYWx1ZUZpZWxkBQtEaXN0cmljdF9JRB4LXyFE YXRhQm91bmRnZBAVDR5TcmlrYWt1bGFtICAgICAgICAgICAgICAgICAgICAeVml6aWFuYWdhcmFtICAgICAgICAgI CAgICAgICAgHlZpc2FraGFwYXRuYW0gICAgICAgICAgICAgICAgIB5FYXN0IEdvZGF2YXJpICAgICAgICAgICAgIC AgICAeV2VzdCBHb2RhdmFyaSAgICAgICAgICAgICAgICAgHktyaXNobmEgICAgICAgICAgICAgICAgICAgICAgICAgIB5 HdW50dXIgICAgICAgICAgICAgICAgICAgICAgICAeUHJha2FzYW0gICAgICAgICAgICAgICAgICAgICAgICAgHlNyaSBQ b3R0aSBTcmlyYW11bHUgTmVsbG9yZSAgIB5DaG10dG9vciAgICAgICAgICAgICAgICAgICAgICAeWS5TL11uQ3VkZ GFwYWggICAgICAgICAgICAgICAgHkFuYW50aGFwdXIgICAgICAgICAgICAgICAgICAgIB5LdXJub29sICAgICAgICAgIC AgiCAgiCAgiCAgiCAgiCAVDQiwMQiwMgiwMwiwNAiwNQiwNgiwNwiwOAiwOQixMAixMQixMxQrAw1nZ2dnZ2d nZ2dnZ2dnFgFmZAIFDxAPFgYfAAUHU3RhdGlvbh8BBQlTdGF0aW9uSUQfAmdkEBUBUlNBTUtSRyBQaXN0b24gUXVh cnRlcnMsIFB5ZGliaGVlbWF2YXJhbSAoViksICBSYW5hc3RhbGFtIChNKSwgU3Jpa2FrdWxhbSBEaXN0cmljdC4VA QIxMBQrAwFnFgFmZAIIDzwrABECAA8WBB8CZx4LXyFJdGVtQ291bnQCCWQMFCsACBYIHgROYW11BQRZZWFyHgpJc1 JlYWRPbmx5aB4EVHlwZRkrAR4JRGF0YUZpZWxkBQRZZWFyFggfBAUIQ2F0ZWdvcnkfBWgfBhkrAh8HBQhDYXRlZ29 yeRYIHwQFBFBNMTAfBWqfBhkrAh8HBQRQTTEwFqqfBAUEUE0yNR8FaB8GGSsCHwcFBFBNMjUWCB8EBQNTbzIfBWqf BhkrAh8HBQNTbzIWCB8EBQNObzIfBWqfBhkrAh8HBQNObzIWCB8EBQNOSDMfBWqfBhkrAh8HBQNOSDMWCB8EBQJDT x8FaB8GGSsCHwcFAkNPFgJmD2QWFgIBD2QWDAICDw8WAh4EVGV4dAUdUlNQTSA8YnIvPiBQTSgxMCkgPGJyLz4gdW cvbTNkZAIDDw8WAh8IBRJQTSqyNSkqPGJyLz4qdWcvbTNkZAIEDw8WAh8IBQ9TTzIqPGJyLz4qdWcvbTNkZAIFDw8 WAh8IBQ9OTzIqPGJyLz4qdWcvbTNkZAIGDw8WAh8IBQ9OSDMqPGJyLz4qdWcvbTNkZAIHDw8WAh8IBQ5DTyA8YnIv PiBtZy9tM2RkAgIPZBYQZg8PFgIfCAUEMjAxMWRkAgEPDxYEHwgFCkluZHVzdHJpYWweB1Jvd1NwYW4CCGRkAgIPD xYCHwqFAjU0ZGQCAw8PFqIfCAUBLWRkAqQPDxYCHwqFAS1kZAIFDw8WAh8IBQEtZGQCBq8PFqIfCAUBLWRkAqcPDx YCHwgFAS1kZAIDD2QWEGYPDxYCHwgFBDIwMTJkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCBx4HVmlzaWJsZWhkZAI CDw8WAh8IBQEtZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFAS1kZAIFDw8WAh8IBQEtZGQCBg8PFgIfCAUBLWRkAgcP DxYCHwgFAS1kZAIED2QWEGYPDxYCHwgFBDIwMTNkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCBh8KaGRkAgIPDxYCH wqFAjc2ZGQCAw8PFqIfCAUBLWRkAqQPDxYCHwqFBDExLjFkZAIFDw8WAh8IBQQxNi45ZGQCBq8PFqIfCAUCMjhkZA IHDw8WAh8IBQEtZGQCBQ9kFhBmDw8WAh8IBQQyMDE0ZGQCAQ8PFgYfCAUKSW5kdXN0cmlhbB8JAgUfCmhkZAICDw8 WAh8IBQI2OWRkAgMPDxYCHwgFAS1kZAIEDw8WAh8IBQQxNC40ZGQCBQ8PFgIfCAUCMjJkZAIGDw8WAh8IBQI10GRk AgcPDxYCHwgFAS1kZAIGD2QWEGYPDxYCHwgFBDIwMTVkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCBB8KaGRkAgIPD xYCHwgFAjcyZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFAzkuN2RkAgUPDxYCHwgFBDIyLjJkZAIGDw8WAh8IBQI2Nm PDxYCHwqFAjcyZGQCAw8PFqIfCAUBLWRkAqQPDxYCHwqFAzquNmRkAqUPDxYCHwqFBDE5LjdkZAIGDw8WAh8IBQI3 MWRkAgcPDxYCHwgFAS1kZAIID2QWEGYPDxYCHwgFBDIwMTdkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCAh8KaGRkA gIPDxYCHwgFAjY5ZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFAzguNWRkAgUPDxYCHwgFBDE4LjFkZAIGDw8WAh8IBQ I2OWRkAgcPDxYCHwgFAS1kZAIJD2QWEGYPDxYCHwgFBDIwMThkZAIBDw8WBB8IBQpJbmR1c3RyaWFsHwpoZGQCAg8 PFGIfCAUCNzRkZAIDDw8WAh8IBQEtZGQCBA8PFGIfCAUEMTAuN2RkAgUPDxYCHwgFBDIwLjRkZAIGDw8WAh8IBQI3 MmRkAgcPDxYCHwgFAS1kZAIKD2QWEGYPDxYCHwgFBiZuYnNwO2RkAgEPDxYCHwgFG1N0YW5kYXJkcyAoQW5udWFsI EF2ZXJhZ2VzKWRkAqIPDxYCHwgFAjYwZGQCAw8PFqIfCAUCNDBkZAIEDw8WAh8IBQI1MGRkAqUPDxYCHwgFAjQwZG QCBg8PFgIfCAUDMTAwZGQCBw8PFgIfCAUBMmRkAgsPDxYCHwpoZGQCCg88KwARAgAPFgQfAmcfAwIFZAwUKwAJFgg fBAUEWWVhch8FaB8GGSsBHwcFBF11YXIWCB8EBQpNb250aF9uYW11HwVoHwYZKwIfBwUKTW9udGhfbmFtZRYIHwQF CENhdGVnb3J5HwVoHwYZKwIfBwUIQ2F0ZWdvcnkWCB8EBQRQTTEwHwVoHwYZKwIfBwUEUE0xMBYIHwQFBFBNMjUfB WgfBhkrAh8HBQRQTTI1FggfBAUDU28yHwVoHwYZKwIfBwUDU28yFggfBAUDTm8yHwVoHwYZKwIfBwUDTm8yFggfBA

UDTkgzHwVoHwYZKwIfBwUDTkgzFggfBAUCQ08fBWgfBhkrAh8HBQJDTxYCZg9kFg4CAQ9kFgwCAw8PFgIfCAUdUlN QTSA8YnIvPiBQTSgxMCkgPGJyLz4gdWcvbTNkZAIEDw8WAh8IBRJQTSgyNSkgPGJyLz4gdWcvbTNkZAIFDw8WAh8I BQ9TTzIgPGJyLz4gdWcvbTNkZAIGDw8WAh8IBQ9OTzIgPGJyLz4gdWcvbTNkZAIHDw8WAh8IBQ9OSDMgPGJyLz4gd WcvbTNkZAIIDw8WAh8IBQ5DTyA8YnIvPiBtZy9tM2RkAgIPZBYSZg8PFgIfCAUEMjAxOWRkAgEPDxYCHwgFB0phbn VhcnlkZAICDw8WBB8IBQpJbmR1c3RyaWFsHwkCBGRkAgMPDxYCHwgFAjc1ZGQCBA8PFgIfCAUCNDRkZAIFDw8WAh8 IBQIxMGRkAqYPDxYCHwqFBDE5LjJkZAIHDw8WAh8IBQI3N2RkAqqPDxYCHwqFAS1kZAIDD2QWEmYPDxYCHwqFBDIw MTlkZAIBDw8WAh8IBQhGZWJydWFyeWRkAqIPDxYGHwqFCkluZHVzdHJpYWwfCQIDHwpoZGQCAw8PFqIfCAUCNzNkZ AIEDw8WAh8IBQI0MmRkAgUPDxYCHwgFAThkZAIGDw8WAh8IBQQxOS4yZGQCBw8PFgIfCAUCNzZkZAIIDw8WAh8IBQ EtZGQCBA9kFhJmDw8WAh8IBQQyMDE5ZGQCAQ8PFgIfCAUFTWFyY2hkZAICDw8WBh8IBQpJbmR1c3RyaWFsHwkCAh8 KaGRkAgMPDxYCHwgFAjc0ZGQCBA8PFgIfCAUCNDBkZAIFDw8WAh8IBQE4ZGQCBg8PFgIfCAUEMTkuMmRkAgcPDxYC HwgFAjczZGQCCA8PFgIfCAUBLWRkAgUPZBYSZg8PFgIfCAUEMjAxOWRkAgEPDxYCHwgFBUFwcmlsZGQCAg8PFgQfC AUKSW5kdXN0cmlhbB8KaGRkAgMPDxYCHwgFAjc2ZGQCBA8PFgIfCAUCMzhkZAIFDw8WAh8IBQIxMGRkAgYPDxYCHw qFBDE5LjJkZAIHDw8WAh8IBQI3MmRkAqqPDxYCHwqFAS1kZAIGD2QWEmYPDxYCHwqFBiZuYnNwO2RkAqEPDxYCHwq BA8PFgIfCAUCNjBkZAIFDw8WAh8IBQI4MGRkAgYPDxYCHwgFAjgwZGQCBw8PFgIfCAUDNDAwZGQCCA8PFgIfCAUBN GRkAgcPDxYCHwpoZGQYAgUDZ3YyDzwrAAwBCAIBZAUDZ3YxDzwrAAwBCAIBZPY6sQTr2//4GCtozT88ydhuRBaNro yjc3Zj4Oi0irdu& VIEWSTATEGENERATOR=6C3A295F&ddlDistricts=12345'"\'\");|]*%00{%0d%0a<%00> bf%27' \mathbf{Q} &ddlStations=10

/pollutioncb/nationaa_ambient_air_quality_monitoring.aspx

Details

URL encoded POST input ddlStations 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 /pollutioncb/nationaa ambient air quality monitoring.aspx HTTP/1.1

Content-Type: application/x-www-form-urlencoded
Referer: https://tptuat.aponline.gov.in/pollutioncb/

Connection: keep-alive

Cookie: ASP.NET_SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate

Content-Length: 5544

Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

EVENTARGUMENT=1& EVENTTARGET=1& EVENTVALIDATION=/wEdABEr5oyvUatJpi5ZCqLhk/JmSfCvlfoVl L48NcRF2wf9Vsj7NjLk8E6yomFtP41os9MN4dWy6i45xDdsiJrG2UcdsqeiyN3hqi5atA1mQ%2ByHpjghHqp60UD3 Qie30xeyGAzi2GjZW84wacFC1nLsuZgpRRu047jLP1I5Qvs%2BZpfv9s50CEGQsQdZ6hoeA6M4Tbl0uWjViXg//oK P/ZA4tTFPDqlvECgA%2Bz00bCqquHMzDGCJedmBD1SP1RChwQbdMkORBBqBfUvlUnHqajrJLqh0EtCNEQYsonxWI2 tv/9FTNHa54/aXozq3BrzdY51OG4uudg%2BoI0FBgv5kfHepmIrudNuzUDROkL2sq6dXDTi6WVc7WBe6C60EB93gm c2KThRAKG2OuGNL9J5qQWsuKO7e& LASTFOCUS=1& VIEWSTATE=/wEPDwULLTE0NTIwNjExNzAPZBYCAqMPZBY IAgMPEA8WBh4NRGF0YVRleHRGaWVsZAUIRG1zdHJpY3QeDkRhdGFWYWx1ZUZpZWxkBQtEaXN0cmljdF9JRB4LXyFE YXRhQm91bmRnZBAVDR5TcmlrYWt1bGFtICAqICAqICAqICAqICAqICAqICAqICAeVml6aWFuYWdhcmFtICAqICAqICAqI CAgICAgICAgHlZpc2FraGFwYXRuYW0gICAgICAgICAgICAgIB5FYXN0IEdvZGF2YXJpICAgICAgICAgICAgIC AgICAeV2VzdCBHb2RhdmFyaSAgICAgICAgICAgICAgICAgHktyaXNobmEgICAgICAgICAgICAgICAgICAgICAgICAgIB5 HdW50dXIgICAgICAgICAgICAgICAgICAgICAgICAeUHJha2FzYW0gICAgICAgICAgICAgICAgICAgICAgICAgHlNyaSBQ GFwYWggICAgICAgICAgICAgICAgHkFuYW50aGFwdXIgICAgICAgICAgICAgICAgICAgIB5LdXJub29sICAgICAgICAgIC AqICAqICAqICAqICAQICAVDQIwMQIwMwIwNAIwNQIwNwIwNAIwOAIwOQIxMAIxMQIxMxQrAw1nZ2dnZ2d cnRlcnMsIFB5ZGliaGVlbWF2YXJhbSAoViksICBSYW5hc3RhbGFtIChNKSwgU3Jpa2FrdWxhbSBEaXN0cmljdC4VA QIxMBQrAwFnFgFmZAIIDzwrABECAA8WBB8CZx4LXyFJdGVtQ291bnQCCWQMFCsACBYIHgROYW11BQRZZWFyHgpJc1 JlYWRPbmx5aB4EVHlwZRkrAR4JRGF0YUZpZWxkBQRZZWFyFggfBAUIQ2F0ZWdvcnkfBWgfBhkrAh8HBQhDYXRlZ29 yeRYIHwQFBFBNMTAfBWgfBhkrAh8HBQRQTTEwFggfBAUEUE0yNR8FaB8GGSsCHwcFBFBNMjUWCB8EBQNTbzIfBWgf BhkrAh8HBQNTbzIWCB8EBQNObzIfBWgfBhkrAh8HBQNObzIWCB8EBQNOSDMfBWgfBhkrAh8HBQNOSDMWCB8EBQJDT x8FaB8GGSsCHwcFAkNPFgJmD2QWFgIBD2QWDAICDw8WAh4EVGV4dAUdUlNQTSA8YnIvPiBQTSgxMCkgPGJyLz4gdW cvbTNkZAIDDw8WAh8IBRJQTSgyNSkgPGJyLz4gdWcvbTNkZAIEDw8WAh8IBQ9TTzIgPGJyLz4gdWcvbTNkZAIFDw8 WAh8IBQ9OTzIgPGJyLz4gdWcvbTNkZAIGDw8WAh8IBQ9OSDMgPGJyLz4gdWcvbTNkZAIHDw8WAh8IBQ5DTyA8YnIv PiBtZy9tM2RkAgIPZBYQZg8PFgIfCAUEMjAxMWRkAgEPDxYEHwgFCkluZHVzdHJpYWweB1Jvd1NwYW4CCGRkAgIPD

xYCHwgFAjU0ZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFAS1kZAIFDw8WAh8IBQEtZGQCBg8PFgIfCAUBLWRkAgcPDx YCHwgFAS1kZAIDD2QWEGYPDxYCHwgFBDIwMTJkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCBx4HVmlzaWJsZWhkZAI CDw8WAh8IBQEtZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFAS1kZAIFDw8WAh8IBQEtZGQCBg8PFgIfCAUBLWRkAgcP DxYCHwgFAS1kZAIED2QWEGYPDxYCHwgFBDIwMTNkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCBh8KaGRkAgIPDxYCH wgFAjc2ZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFBDExLjFkZAIFDw8WAh8IBQQxNi45ZGQCBg8PFgIfCAUCMjhkZA IHDw8WAh8IBQEtZGQCBQ9kFhBmDw8WAh8IBQQyMDE0ZGQCAQ8PFqYfCAUKSW5kdXN0cmlhbB8JAqUfCmhkZAICDw8 WAh8IBQI2OWRkAgMPDxYCHwgFAS1kZAIEDw8WAh8IBQQxNC40ZGQCBQ8PFgIfCAUCMjJkZAIGDw8WAh8IBQI1OGRk AgcPDxYCHwgFAS1kZAIGD2QWEGYPDxYCHwgFBDIwMTVkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCBB8KaGRkAgIPD xYCHwgFAjcyZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFAzkuN2RkAgUPDxYCHwgFBDIyLjJkZAIGDw8WAh8IBQI2Nm ${\tt RkAgcPDxYCHwgFAS1kZAIHD2QWEGYPDxYCHwgFBDIwMTZkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCAx8KaGRkAgII}$ PDxYCHwgFAjcyZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFAzguNmRkAgUPDxYCHwgFBDE5LjdkZAIGDw8WAh8IBQI3 MWRkAgcPDxYCHwgFAS1kZAIID2QWEGYPDxYCHwgFBDIwMTdkZAIBDw8WBh8IBQpJbmR1c3RyaWFsHwkCAh8KaGRkA gIPDxYCHwgFAjY5ZGQCAw8PFgIfCAUBLWRkAgQPDxYCHwgFAzguNWRkAgUPDxYCHwgFBDE4LjFkZAIGDw8WAh8IBQ I2OWRkAqcPDxYCHwqFAS1kZAIJD2QWEGYPDxYCHwqFBDIwMThkZAIBDw8WBB8IBQpJbmR1c3RyaWFsHwpoZGQCAq8 PFqIfCAUCNzRkZAIDDw8WAh8IBQEtZGQCBA8PFqIfCAUEMTAuN2RkAqUPDxYCHwqFBDIwLjRkZAIGDw8WAh8IBQI3 MmRkAgcPDxYCHwgFAS1kZAIKD2QWEGYPDxYCHwgFBiZuYnNwO2RkAgEPDxYCHwgFG1N0YW5kYXJkcyAoQW5udWFsI EF2ZXJhZ2VzKWRkAgIPDxYCHwgFAjYwZGQCAw8PFgIfCAUCNDBkZAIEDw8WAh8IBQI1MGRkAgUPDxYCHwgFAjQwZG QCBg8PFgIfCAUDMTAwZGQCBw8PFgIfCAUBMmRkAgsPDxYCHwpoZGQCCg88KwARAgAPFgQfAmcfAwIFZAwUKwAJFgg fBAUEWWVhch8FaB8GGSsBHwcFBF11YXIWCB8EBQpNb250aF9uYW11HwVoHwYZKwIfBwUKTW9udGhfbmFtZRYIHwQF CENhdGVnb3J5HwVoHwYZKwIfBwUIQ2F0ZWdvcnkWCB8EBQRQTTEwHwVoHwYZKwIfBwUEUE0xMBYIHwQFBFBNMjUfB WqfBhkrAh8HBQRQTTI1FqqfBAUDU28yHwVoHwYZKwIfBwUDU28yFggfBAUDTm8yHwVoHwYZKwIfBwUDTm8yFggfBA UDTkgzHwVoHwYZKwIfBwUDTkgzFggfBAUCQ08fBWgfBhkrAh8HBQJDTxYCZg9kFg4CAQ9kFgwCAw8PFgIfCAUdUlN QTSA8YnIvPiBQTSqxMCkqPGJyLz4qdWcvbTNkZAIEDw8WAh8IBRJQTSqyNSkqPGJyLz4qdWcvbTNkZAIFDw8WAh8I BQ9TTzIgPGJyLz4gdWcvbTNkZAIGDw8WAh8IBQ9OTzIgPGJyLz4gdWcvbTNkZAIHDw8WAh8IBQ9OSDMgPGJyLz4gd WcvbTNkZAIIDw8WAh8IBQ5DTyA8YnIvPiBtZy9tM2RkAgIPZBYSZg8PFgIfCAUEMjAxOWRkAgEPDxYCHwgFB0phbn VhcnlkZAICDw8WBB8IBQpJbmR1c3RyaWFsHwkCBGRkAgMPDxYCHwgFAjc1ZGQCBA8PFgIfCAUCNDRkZAIFDw8WAh8 IBQIxMGRkAqYPDxYCHwqFBDE5LjJkZAIHDw8WAh8IBQI3N2RkAqqPDxYCHwqFAS1kZAIDD2QWEmYPDxYCHwqFBDIw MTlkZAIBDw8WAh8IBQhGZWJydWFyeWRkAgIPDxYGHwgFCkluZHVzdHJpYWwfCQIDHwpoZGQCAw8PFgIfCAUCNzNkZ AIEDw8WAh8IBQI0MmRkAgUPDxYCHwgFAThkZAIGDw8WAh8IBQQxOS4yZGQCBw8PFgIfCAUCNzZkZAIIDw8WAh8IBQ EtZGQCBA9kFhJmDw8WAh8IBQQyMDE5ZGQCAQ8PFgIfCAUFTWFyY2hkZAICDw8WBh8IBQpJbmR1c3RyaWFsHwkCAh8 KaGRkAgMPDxYCHwgFAjc0ZGQCBA8PFgIfCAUCNDBkZAIFDw8WAh8IBQE4ZGQCBg8PFgIfCAUEMTkuMmRkAgcPDxYC HwgFAjczZGQCCA8PFgIfCAUBLWRkAgUPZBYSZg8PFgIfCAUEMjAxOWRkAgEPDxYCHwgFBUFwcmlsZGQCAg8PFgQfC AUKSW5kdXN0cmlhbB8KaGRkAqMPDxYCHwqFAjc2ZGQCBA8PFqIfCAUCMzhkZAIFDw8WAh8IBQIxMGRkAqYPDxYCHw gFBDE5LjJkZAIHDw8WAh8IBQI3MmRkAggPDxYCHwgFAS1kZAIGD2QWEmYPDxYCHwgFBiZuYnNwO2RkAgEPDxYCHwg FBiZuYnNwO2RkAgIPDxYCHwgFHVNOYW5kYXJkcyAoMjQgaG91cnMgQXZ1cmFnZXMpZGQCAw8PFgIfCAUDMTAwZGQC BA8PFgIfCAUCNjBkZAIFDw8WAh8IBQI4MGRkAgYPDxYCHwgFAjgwZGQCBw8PFgIfCAUDNDAwZGQCCA8PFgIfCAUBN GRkAgcPDxYCHwpoZGQYAgUDZ3YyDzwrAAwBCAIBZAUDZ3YxDzwrAAwBCAIBZPY6sQTr2//4GCtozT88ydhuRBaNro yjc3Zj4Oi0irdu& VIEWSTATEGENERATOR=6C3A295F&ddlDistricts=01&ddlStations=12345'"\'\");|]* \$00{\$0d\$0a<\$00>\$bf\$27' Ω

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:

<machineKev validation="AES"/>

Affected items

Web Server

Details

Request headers

```
GET /pollutioncb/feedback.aspx HTTP/1.1
```

Cookie: ASP.NET SessionId=uilu1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

/pollutioncb/a_external_advisory_committe_New.aspx

Details

Request headers

```
GET /pollutioncb/a_external_advisory_committe_New.aspx HTTP/1.1
```

Cookie: ASP.NET SessionId=pm3hctz3hupfk1ymhu2ii5qw

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

/pollutioncb/a_real_time_noise_monitoring_stations.aspx

Details

Request headers

GET /pollutioncb/a real time noise monitoring stations.aspx HTTP/1.1

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

/pollutioncb/content-management-cfe.aspx

Details

Request headers

POST /pollutioncb/content-management-cfe.aspx HTTP/1.1

Content-Type: application/x-www-form-urlencoded Cookie: ASP.NET SessionId=uilulct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate

Content-Length: 114

Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

__VIEWSTATE=/wEPDwULLTEzODAzNzU2NDZkZBWNRH%2B2%2BKM4wklMC0q3SA2BWm/lV30jX25P1WfyMbhd&__VIEWSTATEGENERATOR=353F5F28

/pollutioncb/content-management-cfo.aspx

Details

GET /pollutioncb/content-management-cfo.aspx HTTP/1.1

Referer: https://www.google.com/search?hl=en&q=testing

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

Connection: Keep-alive

/pollutioncb/continuous-ambient-air-quality-monitoring-stations-caaqms.aspx

Details

Request headers

GET /pollutioncb/continuous-ambient-air-quality-monitoring-stations-caaqms.aspx HTTP/1.1

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

/pollutioncb/feedback.aspx

Details

Request headers

GET /pollutioncb/feedback.aspx HTTP/1.1

Cookie: ASP.NET SessionId=pm3hctz3hupfk1ymhu2ii5qw

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

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

<u>HttpRuntimeSection.EnableVersionHeader Property (http://msdn.microsoft.com/enus/library/system.web.configuration.httpruntimesection.enableversionheader.aspx)</u>

Affected items

Web Server

Details

Version information found:

4.0.30319

Request headers

GET /|~.aspx HTTP/1.1 Connection: keep-alive

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Olickjacking: 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. Consult Web references for more information about the possible values for this header.

References

<u>The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)</u>

Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)

OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)

<u>Defending with Content Security Policy frame-ancestors directive</u>

(https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frameancestors_directive)

Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-code-needed)

Affected items

Web Server

Details

Request headers

GET / HTTP/1.1

Connection: keep-alive

Cookie: ASP.NET SessionId=pm3hctz3hupfk1ymhu2ii5qw

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Possible sensitive directories

Severity	Low
Reported by module	/Scripts/PerFolder/Possible_Sensitive_Directories.script

Description

A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

Web Server Security and Database Server Security (http://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

Web Server

Details

Request headers

GET /pollutioncb/uploads HTTP/1.1

Accept: acunetix/wvs Range: bytes=0-99999 Connection: keep-alive

Cookie: ASP.NET SessionId=ui1u1ct4zaj025knmoddhubf

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

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.

Affected items

/pollutioncb/AppointmentMS.aspx

Details

POST /pollutioncb/AppointmentMS.aspx HTTP/1.1 Content-Type: application/x-www-form-urlencoded Cookie: ASP.NET SessionId=uilulct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate

Content-Length: 1727

Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

EVENTVALIDATION=/wEdABp/vaanXNMTbZclx2Luly/1JGAFvP3BWIYdnqm0xGD33hffPEYN0Gr%2B8o/R36bDn DoJ8f01hK1tIAud3QCqieFtV6ItGWtk/kC83AupZud3nLway05GmvzqD/esPsVzqRcTV2Yd7dvrU47ouI8JLz1HEx IA608hWwIWORKCudq9qVPC55siuOfYvXn2zJs0YU6NTFqNzNYcj3CTUD0nnR8zauZDiGNqsUq2VT0ADu3BqeHcEqJ d9wUWvSVqjtUL9qJCnLEzADTFxrML8S8XzLr8HNLcCfRk48iVzk64o4qWLFvrQXKHGRPJi1DZ4aaHXnaaQRNj27JB RdBAmQI9QHVddap7eM06KOJY0n9H1tNS4nJnJn/4UdbTlCbihLSSSuTYEojgdGq3Mu8Lu0xZ8QsdwsQHZSgtak0Gc kVf30r3B3ZawmrS7mAaCEircaMTjVasEpMGhMrWor0WDE0xpvK4%2BQID2tpjfSbwT6WuVmLKZjsvgabDL71Ho8Un Fk4gIY3/H1A8JePMN6iGHckUTZUZPOaW1pQztoQA36D1w/%2BbXUIi7FK5z70XmmUAb8SHCvzhG01Hbb0gf0tkeBt 9aAoE& VIEWSTATE=/wEPDwUIMzY4MDY5MzUPZBYCAgMPZBYCAgMPEA8WBh4NRGF0YVRleHRGaWVsZAUUZGlzdHJ pY3RfZGVzY3JpcHRpb24eDkRhdGFWYWx1ZUZpZWxkBQtkaXN0cmljdF9pZB4LXyFEYXRhQm91bmRnZBAVDqZTZWxl Y3QeU3Jpa2FrdWxhbSAgICAgICAgICAgICAgICAgICAgICAgHlZpemlhbmFnYXJhbSAgICAgICAgICAgICAgIB5Wa XNha2hhcGF0bmFtICAgICAgICAgICAgICAgICAeRWFzdCBHb2RhdmFyaSAgICAgICAgICAgICAgICAgHldlc3QgR2 9kYXZhcmkgICAgICAgICAgICAgICAgIB5LcmlzaG5hICAgICAgICAgICAgICAgICAgICAgICAeR3VudHVyICAgICA gICAgICAgICAgICAgICAgICAgHlByYWthc2FtICAgICAgICAgICAgICAgICAgICAgIB5TcmkgUG90dGkgU3JpcmFt dWx1IE5lbGxvcmUgICAeQ2hpdHRvb3IgICAgICAgICAgICAgICAgICAgICAgICAgHlkuUy5SLiAgICAgICAgICAgICAgI CAqICAqICAqIB5BbmFudGhhcHVyYW111CAqICAqICAqICAqICAqICAeS3Vybm9vbCAqICAqICAqICAqICAqICAqICAqIC kZGQht64Wr5uU8XjDUREjqNuvndayjLI/63ZAMX9pO5OnFw==& VIEWSTATEGENERATOR=0A3DDF53&btnSubmit =Submit&ddldist=00&rdoappoint=01&txtdateofvisite=http://www.vulnweb.com&txtdesignation=1& txtemail=sample%40email.tst&txtmobilenumber=987-65-

/pollutioncb/feedback.aspx

Details

Request headers

POST /pollutioncb/feedback.aspx HTTP/1.1

Content-Type: application/x-www-form-urlencoded Cookie: ASP.NET SessionId=uilulct4zaj025knmoddhubf

Accept: */*

Accept-Encoding: gzip, deflate

Content-Length: 690

Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

4329&txtnameofperson=CpjJwWHV&txtnameofunit=CpjJwWHV&txtpurposeofviste=555

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

 $ImageButton1=1\&_EVENTVALIDATION=/wEdAas7jX9YonL7ZZ6cx9DuyLsOVCDn2pfngd5PS19R1fd0WMjkomTeSEWFH1KGCQje%2BaBnjdbt1ZLOCXGRPBQfNNIqUpniTDrt%2BjARd%2BhUExs4c9gSiOB0arcy7wu7TFnxCx3CxAdlKC1qTQZyRV/fSvcHLd9Mi3j84XpObGQKq4C%2BFs5XhHXFJzWEz/a31vNJ4KXpkAKvH1FmeWUpJ6tT4i4qPOaW1pQztoQA36D1w/%2BbXR2e1AknqONs0occKNnOwBbt0KC0n755T0yxNBJpjPSK&__VIEWSTATE=/wEPDwUKLTI3OTQ3NzE0N2QYAQUeX19Db250cm9sc1JlcXVpcmVQb3N0QmFja0tleV9fFgEFDEltYWdlQnV0dG9uMdew1VSfqJiGWM/vQJwf0lxSwPljGz6ttDACVXA6yvgs&__VIEWSTATEGENERATOR=938AE22F&btnSubmit=Submit&txtaddress=3137%20Laguna%20Street&txtdist=1&txtemail=sample%40email.tst&txtfeedbacksuggition=555&txtimgcode=94102&txtmobilenumber=987-65-4329&txtname=CpjJwWHV&txtstate=NY$

/pollutioncb/homemore.aspx

Details

GET /pollutioncb/homemore.aspx?type=news HTTP/1.1

Cookie: ASP.NET SessionId=pm3hctz3hupfk1ymhu2ii5qw

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

① 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)

Affected items

$/pollutioncb/a_Procedure for Online Connectivity. htm$

Details

Pattern found:

murali.sss@appcb.gov.in

Request headers

/pollutioncb/bio-medical-waste-management.html

Details

Pattern found: rainbowindustries@rocketmail.com maridi_andhra@yahoo.com evbtechmcr@gmail.com safenviron@yahoo.com 2015omw@gmail.com ss.biocare@yahoo.com awm_18@rediffmail.com srivenenviron@gmail.com medicalwastesolutionskurnool@gmail.com uh4_jcee@pcb.ap.gov.in unit4-jcee@appcb.gov.in

Request headers

/pollutioncb/contact-us.html

Details

Pattern found:

```
chairman@appcb.gov.in

membersecy@appcb.gov.in

pa-chairman@appcb.gov.in

pa-ms@appcb.gov.in

chiefengineer@appcb.gov.in

unit1-jcee@appcb.gov.in

unit2-jcee@appcb.gov.in

unit3-jcee@appcb.gov.in

unit4-jcee@appcb.gov.in

senioram@appcb.gov.in

boardlab-jso1@appcb.gov.in
```

Request headers

/pollutioncb/hazardous-waste-management.html

Details

Pattern found:

unit4-jcee@appcb.gov.in

O Possible internal IP address disclosure

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

Description

A string matching an internal IPv4 address was found on this page. This may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

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

Impact

Possible sensitive information disclosure.

Recommendation

Prevent this information from being displayed to the user.

Affected items

/pollutioncb/a_external_advisory_committe_New.aspx	
Details	
Pattern found:	
10.10.18.18	
Request headers	

Subresource Integrity (SRI) not implemented

Severity	Informational
Reported by module	/RPA/SRI_Not_Implemented.js

Description

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha265, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

References

<u>Subresource Integrity (https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)</u>
<u>SRI Hash Generator (https://www.srihash.org/)</u>

Affected items

/pollutioncb/

Details

Request headers

GET /pollutioncb/ HTTP/1.1

Cookie: ASP.NET SessionId=pm3hctz3hupfk1ymhu2ii5qw

Accept: */*

Accept-Encoding: gzip, deflate Host: tptuat.aponline.gov.in

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)

Chrome/41.0.2228.0 Safari/537.21

Connection: Keep-alive

Scanned items (coverage report)

```
https://tptuat.aponline.gov.in/
https://tptuat.aponline.gov.in/pollutioncb/
https://tptuat.aponline.gov.in/pollutioncb/22.03.2017 - Indian Oil Corporation Ltd., (Chennai to Bangalore Pipe line project)
https://tptuat.aponline.gov.in/pollutioncb/a ambient air quality data ap.html
https://tptuat.aponline.gov.in/pollutioncb/a ambient air quality monitoring functions.html
https://tptuat.aponline.gov.in/pollutioncb/a ambient air quality monitoring functions submenu.html
https://tptuat.aponline.gov.in/pollutioncb/a appcb online.html
https://tptuat.aponline.gov.in/pollutioncb/a capacity building.html
https://tptuat.aponline.gov.in/pollutioncb/a categories of industries.html
https://tptuat.aponline.gov.in/pollutioncb/a ConstructionandDemolition.htm
https://tptuat.aponline.gov.in/pollutioncb/a environment acts rules.html
https://tptuat.aponline.gov.in/pollutioncb/a environment standards.html
https://tptuat.aponline.gov.in/pollutioncb/a ewaste management.html
https://tptuat.aponline.gov.in/pollutioncb/a external advisory committe New.aspx
https://tptuat.aponline.gov.in/pollutioncb/a fly ash.html
https://tptuat.aponline.gov.in/pollutioncb/a_green-category.html
https://tptuat.aponline.gov.in/pollutioncb/a guidelines for industries.html
https://tptuat.aponline.gov.in/pollutioncb/a IndestrialWastManagementSystem.htm
https://tptuat.aponline.gov.in/pollutioncb/a Know environment.html
https://tptuat.aponline.gov.in/pollutioncb/a legal action.html
https://tptuat.aponline.gov.in/pollutioncb/a municipal waste management.html
https://tptuat.aponline.gov.in/pollutioncb/a orange-category.html
https://tptuat.aponline.gov.in/pollutioncb/a plastic waste.html
https://tptuat.aponline.gov.in/pollutioncb/a ProcedureforOnlineConnectivity.htm
https://tptuat.aponline.gov.in/pollutioncb/a_real_time_noise_monitoring_stations.aspx
https://tptuat.aponline.gov.in/pollutioncb/a red-category.html
https://tptuat.aponline.gov.in/pollutioncb/a water cess.html
https://tptuat.aponline.gov.in/pollutioncb/a water quality monitoring.html
https://tptuat.aponline.gov.in/pollutioncb/a water quality monitoring functions.html
https://tptuat.aponline.gov.in/pollutioncb/a white category.html
https://tptuat.aponline.gov.in/pollutioncb/achievements.html
https://tptuat.aponline.gov.in/pollutioncb/air quality/
https://tptuat.aponline.gov.in/pollutioncb/ambient-air-quality-monitoring.html
https://tptuat.aponline.gov.in/pollutioncb/Ambient Air Quality Data of AP/
https://tptuat.aponline.gov.in/pollutioncb/Ambient Air Quality Data of AP/SAAQM-DATA-2011-16-and-2017.xlsx
https://tptuat.aponline.gov.in/pollutioncb/annual-reports.html
https://tptuat.aponline.gov.in/pollutioncb/AppointmentMS.aspx
https://tptuat.aponline.gov.in/pollutioncb/Atachments 200519/
https://tptuat.aponline.gov.in/pollutioncb/Atachments 200519/EPH Minutes -31 industries/
https://tptuat.aponline.gov.in/pollutioncb/Atachments 24052019/
https://tptuat.aponline.gov.in/pollutioncb/Atachments 24052019/Guidlines BMW/
https://tptuat.aponline.gov.in/pollutioncb/Atachments 24052019/Guidlines BMW/Guidlines BMW/
https://tptuat.aponline.gov.in/pollutioncb/Atachments 24052019/technical committee meeting/
https://tptuat.aponline.gov.in/pollutioncb/Atachments 24052019/technical committee meeting/technical committee meeting/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 030619/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 06192019/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 070319/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 070319/ewasterul/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 070319/plast/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 070619/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 170519/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 180619/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 220519/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 220519/ephNewPdf's/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 220519/ephPendingPdf's/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 25052019/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 270519/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 270519/BioMedical/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 270519/BioMedical/CommitteMeetings/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 270519/BioMedical/HcfList/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 280519/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 280519/Annual Reports/
```

```
https://tptuat.aponline.gov.in/pollutioncb/Attachments 280519/ClosureOrders-2018-2019/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 280519/ClosuresOrders-2017-2018/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 280519/StopProductionOrders-2017-2018/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 280519/StopProductionOrders-2018-2019/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 280519/StopProductionOrders-2018-2019/Alliance Hydrocarbons -
Cont. SPO - 09.10.18.18
https://tptuat.aponline.gov.in/pollutioncb/Attachments 280619/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2016-2017/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2017-2018/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/44 No of Stone Crushers - Dir -
09.10.18.18
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/EVB Technologies - Dir - 20.08.2018.18
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/Lohiya Edible Oil - Dir - 10.10.2018.18
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/Rainbow Industries - RCO -
05.12.2018.18
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/Rashtriya Ispat - RINS - Dir -
05.12.2018.18
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/South India Krishna Oil, NLR - Dir -
05.12.2018
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/Sri Vijayalakshmi Sago - RSPO
-29.01.2019
https://tptuat.aponline.gov.in/pollutioncb/Attachments 290519/Directions-2018-2019/Trimex sands - Dir - 10.10.18.18
https://tptuat.aponline.gov.in/pollutioncb/Attachments 300519/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 300519/Air Quality/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 31052019/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 31052019/Research fellow-2017/
https://tptuat.aponline.gov.in/pollutioncb/Attachments 31052019/Research fellow-2018/
https://tptuat.aponline.gov.in/pollutioncb/bio-medical-waste-management.html
https://tptuat.aponline.gov.in/pollutioncb/BMW Annual Reports/
https://tptuat.aponline.gov.in/pollutioncb/BMW/
https://tptuat.aponline.gov.in/pollutioncb/board-members.html
https://tptuat.aponline.gov.in/pollutioncb/CalenderJS/
https://tptuat.aponline.gov.in/pollutioncb/CalenderJS/jquery-1.9.1.js
https://tptuat.aponline.gov.in/pollutioncb/CalenderJS/jquery-ui-1.8.19.custom.css
https://tptuat.aponline.gov.in/pollutioncb/CalenderJS/jquery.ui.core.js
https://tptuat.aponline.gov.in/pollutioncb/CalenderJS/jquery.ui.datepicker.js
https://tptuat.aponline.gov.in/pollutioncb/CalenderJS/jquery.ui.widget.js
https://tptuat.aponline.gov.in/pollutioncb/CEPI.html
https://tptuat.aponline.gov.in/pollutioncb/cess.html
https://tptuat.aponline.gov.in/pollutioncb/CFE - Meting pdf/
https://tptuat.aponline.gov.in/pollutioncb/CFE - Meting pdf/Minutes of CFE Committee Meetings 2016/
https://tptuat.aponline.gov.in/pollutioncb/CFE - Meting pdf/Minutes of CFE Committee Meetings 2017/
https://tptuat.aponline.gov.in/pollutioncb/CFE - Meting pdf/Minutes of CFE Committee Meetings 2018/
https://tptuat.aponline.gov.in/pollutioncb/CFO - status/
https://tptuat.aponline.gov.in/pollutioncb/CFO Auto Renewals - 2016/
https://tptuat.aponline.gov.in/pollutioncb/CFO Auto Renewals - 2016/CFO-AutoRenew-01.08.2016-Sri-Arunachaleswara-
Granites-Chittoor-Dist.pdf"
https://tptuat.aponline.gov.in/pollutioncb/cfo_orders_issued_in_the_year_2016.htm
https://tptuat.aponline.gov.in/pollutioncb/cfo orders issued in the year 2017.htm
https://tptuat.aponline.gov.in/pollutioncb/cfo_red-category.html
https://tptuat.aponline.gov.in/pollutioncb/citizen-charter-rti.html
https://tptuat.aponline.gov.in/pollutioncb/Committee Meetings/
https://tptuat.aponline.gov.in/pollutioncb/consent-management-consent-for-operation-categories-of-industries.htm
https://tptuat.aponline.gov.in/pollutioncb/consent-management-consent-for-operation-fee-structure.htm
https://tptuat.aponline.gov.in/pollutioncb/consent_management_consent_for_establishment_categories_of_industries_3.htm
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for establishment cfe committee meetings.htm
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for establishment cfe orders issued 3.htm
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for establishment delegation of power.htm
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for establishment fee structure.htm
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for establishment siting criteria.htm
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for operation auto renewals.htm
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for operation consent status.htm
```

```
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for operations cfo committee meetings.htm
https://tptuat.aponline.gov.in/pollutioncb/consent management consent for operationt cfo orders issued.htm
https://tptuat.aponline.gov.in/pollutioncb/ConsentManagementConsentForOperationHowToaApply.htm
https://tptuat.aponline.gov.in/pollutioncb/contact-us.html
https://tptuat.aponline.gov.in/pollutioncb/content-management-cfe-fee.htm
https://tptuat.aponline.gov.in/pollutioncb/content-management-cfe.aspx
https://tptuat.aponline.gov.in/pollutioncb/content-management-cfo-fee.htm
https://tptuat.aponline.gov.in/pollutioncb/content-management-cfo.aspx
https://tptuat.aponline.gov.in/pollutioncb/continuous-ambient-air-quality-monitoring-stations-caaqms.aspx
https://tptuat.aponline.gov.in/pollutioncb/css/
https://tptuat.aponline.gov.in/pollutioncb/css/aswini.css
https://tptuat.aponline.gov.in/pollutioncb/css/bootstrap.min.css
https://tptuat.aponline.gov.in/pollutioncb/css/font-awesome.min.css
https://tptuat.aponline.gov.in/pollutioncb/css/gallery/
https://tptuat.aponline.gov.in/pollutioncb/css/gallery/galleries-shortcodes.css
https://tptuat.aponline.gov.in/pollutioncb/css/gallery/magnific-popup.css
https://tptuat.aponline.gov.in/pollutioncb/css/grid-gallery.min.css
https://tptuat.aponline.gov.in/pollutioncb/css/style.css
https://tptuat.aponline.gov.in/pollutioncb/Delegation/
https://tptuat.aponline.gov.in/pollutioncb/Directions/
https://tptuat.aponline.gov.in/pollutioncb/division_technical-department.html
https://tptuat.aponline.gov.in/pollutioncb/downloads/
https://tptuat.aponline.gov.in/pollutioncb/environmental-awareness.html
https://tptuat.aponline.gov.in/pollutioncb/faqs.htm
https://tptuat.aponline.gov.in/pollutioncb/feedback.aspx
https://tptuat.aponline.gov.in/pollutioncb/fonts/
https://tptuat.aponline.gov.in/pollutioncb/fonts/fontawesome-webfont.woff2
https://tptuat.aponline.gov.in/pollutioncb/fonts/glyphicons-halflings-regular.woff2
https://tptuat.aponline.gov.in/pollutioncb/functions consent for establishment how to apply 2.htm
https://tptuat.aponline.gov.in/pollutioncb/green-category-cfo.html
https://tptuat.aponline.gov.in/pollutioncb/green-category.html
https://tptuat.aponline.gov.in/pollutioncb/hazardous-waste-management.html
https://tptuat.aponline.gov.in/pollutioncb/hazordous/
https://tptuat.aponline.gov.in/pollutioncb/homemore.aspx
https://tptuat.aponline.gov.in/pollutioncb/images/
https://tptuat.aponline.gov.in/pollutioncb/images/CM/
https://tptuat.aponline.gov.in/pollutioncb/images/icon/
https://tptuat.aponline.gov.in/pollutioncb/index.aspx
https://tptuat.aponline.gov.in/pollutioncb/js/
https://tptuat.aponline.gov.in/pollutioncb/js/bootstrap-hover-dropdown.min.js
https://tptuat.aponline.gov.in/pollutioncb/js/bootstrap.min.js
https://tptuat.aponline.gov.in/pollutioncb/js/footer.js
https://tptuat.aponline.gov.in/pollutioncb/js/grid-gallery.min.js
https://tptuat.aponline.gov.in/pollutioncb/js/header.js
https://tptuat.aponline.gov.in/pollutioncb/js/jquery.min.js
https://tptuat.aponline.gov.in/pollutioncb/js/script.js
https://tptuat.aponline.gov.in/pollutioncb/justice-b-seshasayana-reddy-committee-vide-ngt-order-in-oa-no-6062018.html
https://tptuat.aponline.gov.in/pollutioncb/LeaveApplication/
https://tptuat.aponline.gov.in/pollutioncb/LeaveApplication/JS/
https://tptuat.aponline.gov.in/pollutioncb/LeaveApplication/JS/jquery-1.9.1.js
https://tptuat.aponline.gov.in/pollutioncb/LeaveApplication/JS/jquery-ui-1.8.19.custom.css
https://tptuat.aponline.gov.in/pollutioncb/LeaveApplication/JS/jquery.ui.core.js
https://tptuat.aponline.gov.in/pollutioncb/LeaveApplication/JS/jquery.ui.datepicker.js
https://tptuat.aponline.gov.in/pollutioncb/LeaveApplication/JS/jquery.ui.widget.js
https://tptuat.aponline.gov.in/pollutioncb/mandate-general-activities.html
https://tptuat.aponline.gov.in/pollutioncb/nationaa ambient air quality monitoring.aspx
https://tptuat.aponline.gov.in/pollutioncb/ocm.html
https://tptuat.aponline.gov.in/pollutioncb/orange-category-cfo.html
https://tptuat.aponline.gov.in/pollutioncb/orange-category.html
https://tptuat.aponline.gov.in/pollutioncb/overview.html
https://tptuat.aponline.gov.in/pollutioncb/pcbnic1/
https://tptuat.aponline.gov.in/pollutioncb/pcbnic1/pcbnic/
https://tptuat.aponline.gov.in/pollutioncb/pcbpdfs/
https://tptuat.aponline.gov.in/pollutioncb/public-hearings-2.html
```

```
https://tptuat.aponline.gov.in/pollutioncb/PublicGriveance-Complaints.html
https://tptuat.aponline.gov.in/pollutioncb/QualityMonitoring.html
https://tptuat.aponline.gov.in/pollutioncb/red-category-cfo.html
https://tptuat.aponline.gov.in/pollutioncb/red-category.html
https://tptuat.aponline.gov.in/pollutioncb/report/
https://tptuat.aponline.gov.in/pollutioncb/Research Fellowship Scheme.html
https://tptuat.aponline.gov.in/pollutioncb/rules.html
https://tptuat.aponline.gov.in/pollutioncb/scientific-departments-laboratories.html
https://tptuat.aponline.gov.in/pollutioncb/scripts/
https://tptuat.aponline.gov.in/pollutioncb/uh4 jcee@pcb.ap.gov.in
https://tptuat.aponline.gov.in/pollutioncb/Uploads/
https://tptuat.aponline.gov.in/pollutioncb/Uploads/fwdappcblegalcellcorrectionssuggestedtonewappcbw/
https://tptuat.aponline.gov.in/pollutioncb/Views/
https://tptuat.aponline.gov.in/pollutioncb/Views/CFOMeet/
https://tptuat.aponline.gov.in/pollutioncb/Views/CFOMeet/2015/
https://tptuat.aponline.gov.in/pollutioncb/Views/CFOMeet/2016/
https://tptuat.aponline.gov.in/pollutioncb/Views/CFOMeet/2017/
https://tptuat.aponline.gov.in/pollutioncb/Views/CFOMeet/2018/
https://tptuat.aponline.gov.in/pollutioncb/Views/CImage.aspx
https://tptuat.aponline.gov.in/pollutioncb/Views/DOP/
https://tptuat.aponline.gov.in/pollutioncb/Views/External2016/
https://tptuat.aponline.gov.in/pollutioncb/Views/External2017/
https://tptuat.aponline.gov.in/pollutioncb/Views/External2018/
https://tptuat.aponline.gov.in/pollutioncb/Views/justicepage/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/AIRQUALITY/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/AIRQUALITY/2016/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/AIRQUALITY/2017/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/AIRQUALITY/2018/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFE2015/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFE2016/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFE2017/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFE2018/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFE2019/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFO Orders 2016/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFO Orders 2016/cfo orders issued in the year 2016.htm
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFO_Orders_2017/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFO2016/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFO2017/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFOC2015/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFOC2016/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFOC2017/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/CFOC2018/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/EAC2018/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/PublicHearings/
https://tptuat.aponline.gov.in/pollutioncb/Views/PDFs/PublichearingsConducted/
https://tptuat.aponline.gov.in/pollutioncb/Views/PublicHearingsNew/
https://tptuat.aponline.gov.in/pollutioncb/Views/PublicHearingsNew/eph minutes pdf for upload/
https://tptuat.aponline.gov.in/pollutioncb/Views/PublicHearingsNew/eph minutes pdf for upload/eph minutes pdf for upload/
https://tptuat.aponline.gov.in/pollutioncb/Views/Rules/
https://tptuat.aponline.gov.in/pollutioncb/vision.html
https://tptuat.aponline.gov.in/pollutioncb/wastemanagement.html
https://tptuat.aponline.gov.in/pollutioncb/water-quality-status-of-polluted-river-stretches-of-andhra-pradesh.html
https://tptuat.aponline.gov.in/pollutioncb/Water Quality Monitoring/
https://tptuat.aponline.gov.in/pollutioncb/white-category-cfo.html
https://tptuat.aponline.gov.in/pollutioncb/white-category.html
```