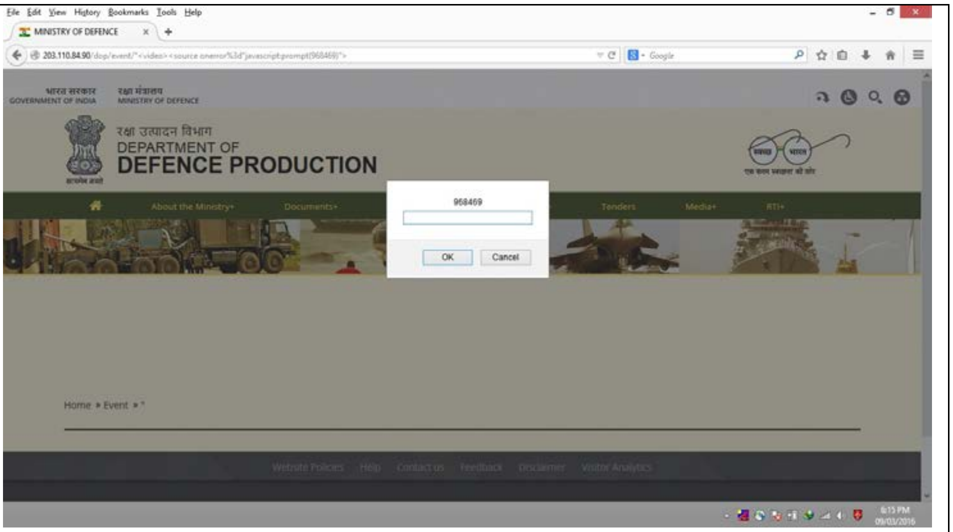
Compliance Audit Findings - Department of Defense Production

1) Vulnerability Title: Cross Site Scripting	
Risk	**High**
Abstract	It was observed that there was a Cross site scripting vulnerability found in the given application
CVE	-----
Ease of Exploitation	Hard
Impact	Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user.
Recommendations	It is recommended to filter out all the following characters at user input: [1] | (pipe sign) [2] & (ampersand sign) [3] ; (semicolon sign) [4] $ (dollar sign) [5] % (percent sign) [6] @ (at sign) [7] ' (single apostrophe) [8] " (quotation mark) [9] \' (backslash-escaped apostrophe) [10] \" (backslash-escaped quotation mark) [11] <> (triangular parenthesis) [12] () (parenthesis) [13] + (plus sign) [14] CR (Carriage return, ASCII 0x0d) [15] LF (Line feed, ASCII 0x0a) [16] , (comma sign) [17] \ (backslash)
Snapshot	1)

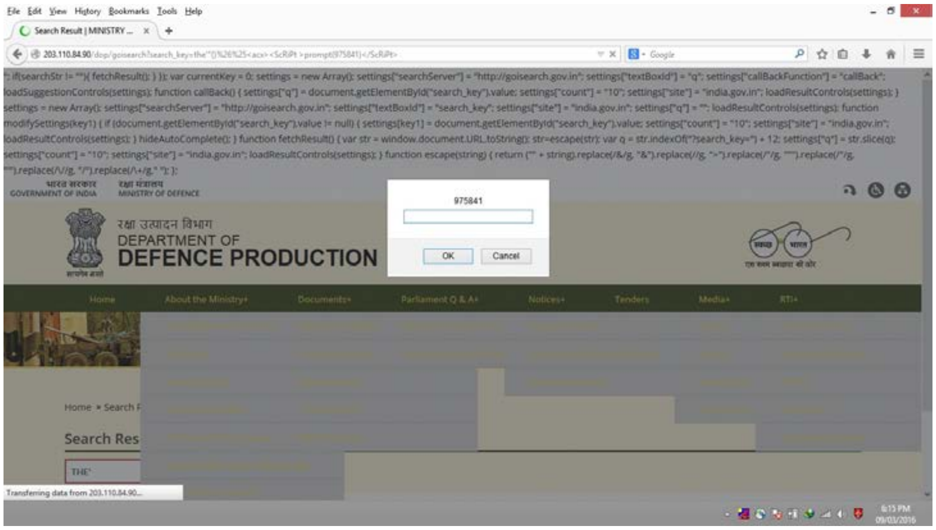


```
203.110.84.90/dop/event/"<video><source onerror%3d"javascript:prompt(968469)">
```

968469

File Edit View History Bookmarks Tools Help
MINISTRY OF DEFENCE
भारत सरकार GOVERNMENT OF INDIA
रक्षा मंत्रालय MINISTRY OF DEFENCE
रक्षा उत्पादन विभाग
DEPARTMENT OF
DEFENCE PRODUCTION
About the Ministry+
Documents+
Tenders
Media+
RTI+
OK
Cancel
Home » Event » "
Website Policies Help Contact us Feedback Disclaimer Visitor Analytics

2)

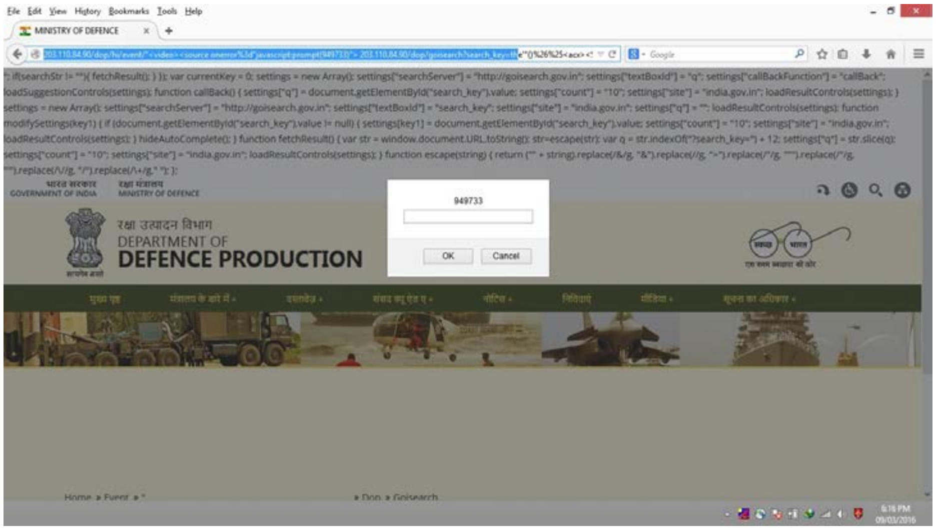


```
203.110.84.90/dop/goisearch?search_key=the"'()%26%25<acx><ScRiPt >prompt(975841)</ScRiPt>
```

```
"; if(searchStr != ""){ fetchResult(); } }); var currentKey = 0; settings = new Array(); settings["searchServer"] = "http://goisearch.gov.in"; settings["textBoxId"] = "q"; settings["callBackFunction"] = "callBack";
loadSuggestionControls(settings); function callBack() { settings["q"] = document.getElementById("search_key").value; settings["count"] = "10"; settings["site"] = "india.gov.in"; loadResultControls(settings); }
settings = new Array(); settings["searchServer"] = "http://goisearch.gov.in"; settings["textBoxId"] = "search_key"; settings["site"] = "india.gov.in"; settings["q"] = ""; loadResultControls(settings); function
modifySettings(key1) { if (document.getElementById("search_key").value != null) { settings[key1] = document.getElementById("search_key").value; settings["count"] = "10"; settings["site"] = "india.gov.in";
loadResultControls(settings); } hideAutoComplete(); } function fetchResult() { var str = window.document.URL.toString(); str=escape(str); var q = str.indexOf("?search_key=") + 12; settings["q"] = str.slice(q);
settings["count"] = "10"; settings["site"] = "india.gov.in"; loadResultControls(settings); } function escape(string) { return ("" + string).replace(/&/g, "&").replace(//g, ">").replace(/"/g, "").replace(/'/g,
"").replace(/\//g, "/").replace(/\+/g," "); };
```

975841

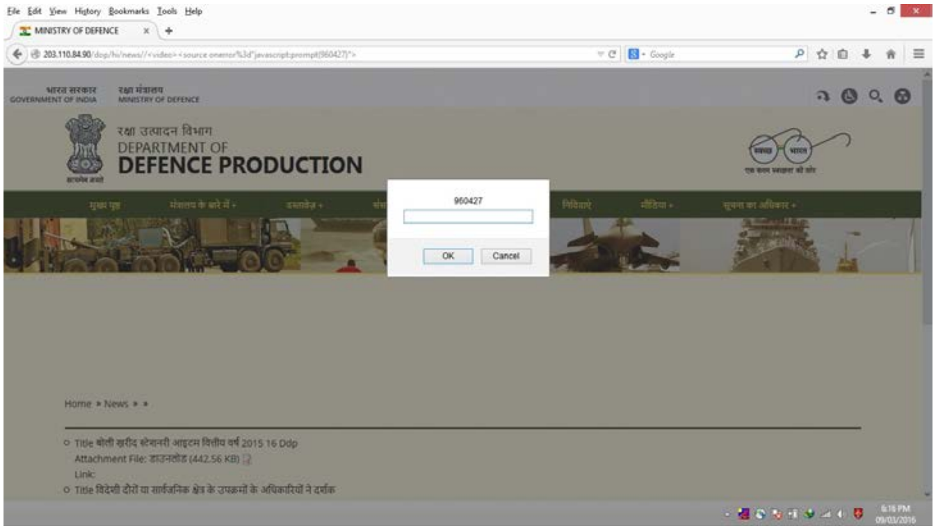
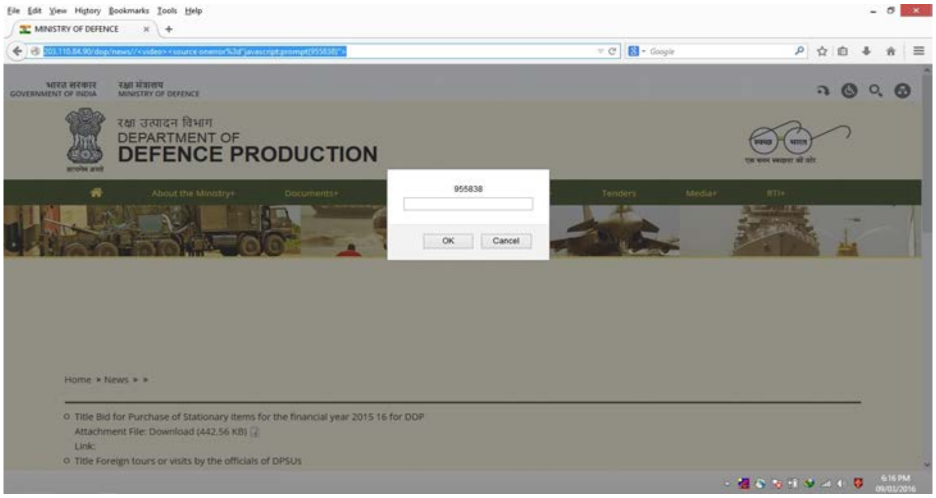
3)

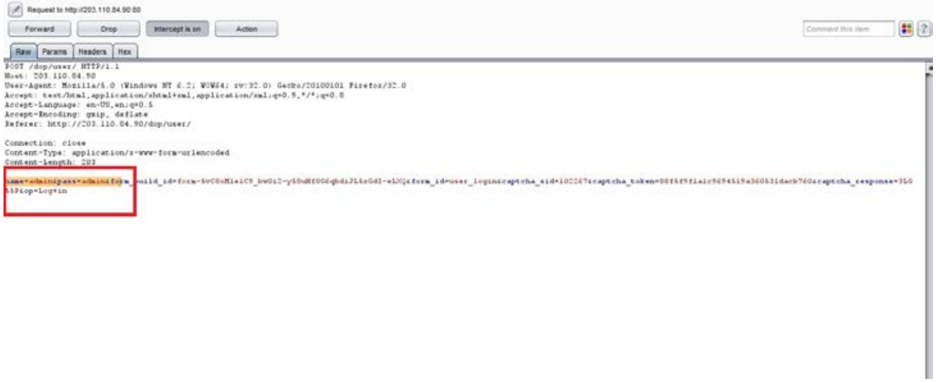


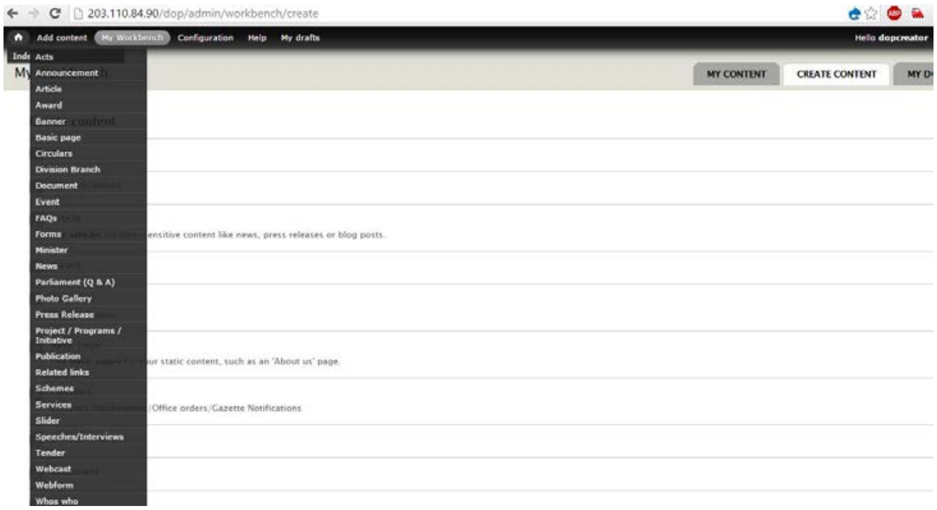
```
203.110.84.90/dop/hi/event/"<video><source onerror%3d"javascript:prompt(949733)"> 203.110.84.90/dop/goisearch?search_key=the"'()%26%25<acx><
```

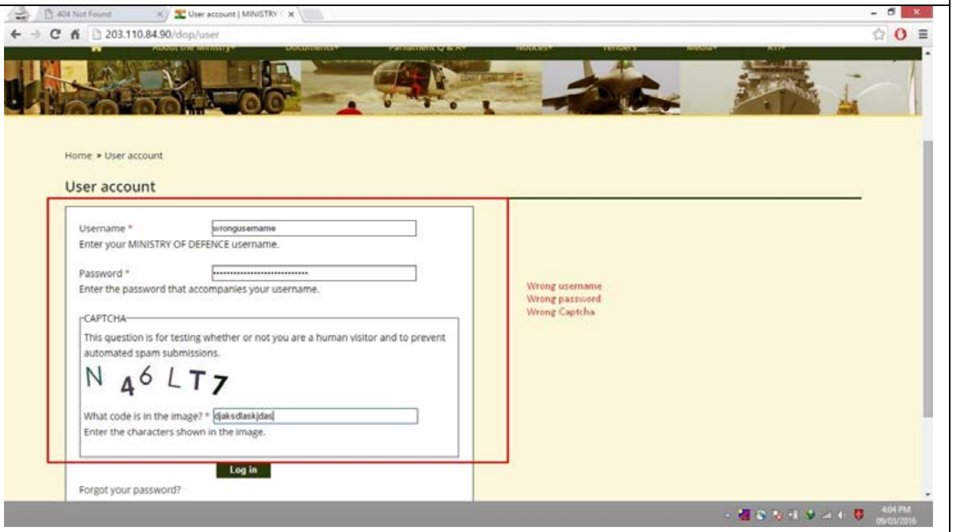
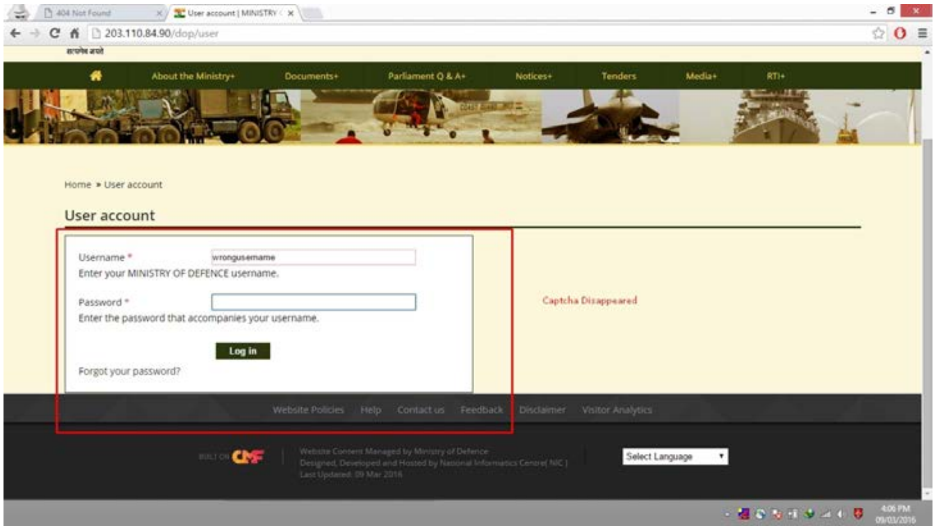
```
"; if(searchStr != ""){ fetchResult(); } }); var currentKey = 0; settings = new Array(); settings["searchServer"] = "http://goisearch.gov.in"; settings["textBoxId"] = "q"; settings["callBackFunction"] = "callBack";
loadSuggestionControls(settings); function callBack() { settings["q"] = document.getElementById("search_key").value; settings["count"] = "10"; settings["site"] = "india.gov.in"; loadResultControls(settings); }
settings = new Array(); settings["searchServer"] = "http://goisearch.gov.in"; settings["textBoxId"] = "search_key"; settings["site"] = "india.gov.in"; settings["q"] = ""; loadResultControls(settings); function
modifySettings(key1) { if (document.getElementById("search_key").value != null) { settings[key1] = document.getElementById("search_key").value; settings["count"] = "10"; settings["site"] = "india.gov.in";
loadResultControls(settings); } hideAutoComplete(); } function fetchResult() { var str = window.document.URL.toString(); str=escape(str); var q = str.indexOf("?search_key=") + 12; settings["q"] = str.slice(q);
settings["count"] = "10"; settings["site"] = "india.gov.in"; loadResultControls(settings); } function escape(string) { return ("" + string).replace(/&/g, "&").replace(//g, ">").replace(/"/g, "").replace(/'/g,
"").replace(/\//g, "/").replace(/\+/g," "); };
```

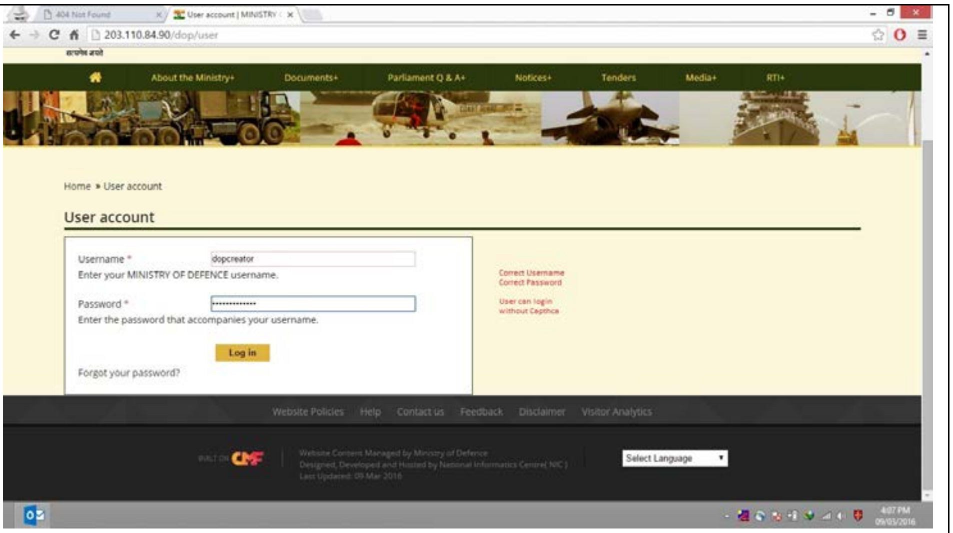
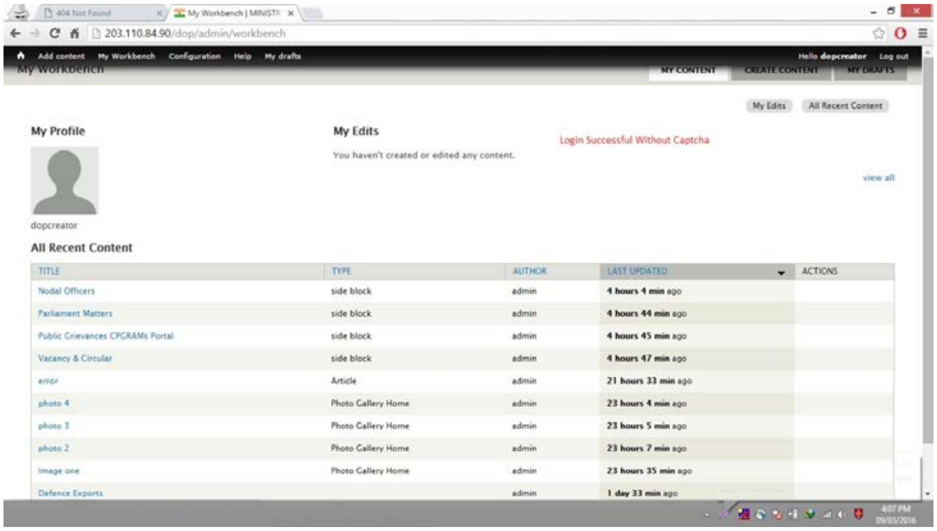
949733

	4)  MINISTRY OF DEFENCE रक्षा उत्पादन विभाग DEPARTMENT OF DEFENCE PRODUCTION 960427 OK Cancel 5)  MINISTRY OF DEFENCE रक्षा उत्पादन विभाग DEPARTMENT OF DEFENCE PRODUCTION 955838 OK Cancel
Affected Site	1) http://203.110.84.90/dop/event/"<video><source%20onerror%3d%22javascript:prompt(968469)%22> 2) http://203.110.84.90/dop/goisearch?search_key=the'%22()%26%25<acx><ScRiPt%20>prompt(975841)</ScRiPt> 3) http://203.110.84.90/dop/hi/event/"<video><source%20onerror%3d%22javascript:prompt(949733)%22> 4) http://203.110.84.90/dop/hi/news//<video><source%20onerror%3d%22javascript:prompt(960427)%22> 5) http://203.110.84.90/dop/news//<video><source%20onerror%3d%22javascript:prompt(955838)%22>
Compliance Status	Not Complied

2) Vulnerability Title: User Credentials Are Sent In Clear Text	
Risk	**Medium**
Abstract	It was observed that the user credentials and debit card details are transmitted over an unencrypted channel.
CVE	-----
Ease of Exploitation	Medium
Impact	A third party may be able to Sniff the user credentials.
Recommendations	It is recommended that User credentials should be transferred to the server over in an Encrypted format.
Snapshot	 Request to http://203.110.84.90:80 Forward Drop Intercept is on Action Raw Params Headers Hex Comment this item POST /dop/user/ HTTP/1.1 Host: 203.110.84.90 User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://203.110.84.90/dop/user/ Connection: close Content-Type: application/x-www-form-urlencoded Content-Length: 203 name=admin&pass=admin&form_build_id=form-5vC0sMleiC9_bw0i2-y50dHf0GdqbdiJL&sGdI-eLXQ&form_id=user_login&captcha_sid=102267&captcha_token=80f5f9f1a1c9d94519a3d0531dacb7d0&captcha_response=3LG 55P&op=Log+in
Affected Site	http://203.110.84.90/dop/user/login
Compliance Status	Not Complied

3) Vulnerability Title: Cookie Expiration and Session expiration not set	
Risk	**Medium**
Abstract	It was observed that cookie expiration time was not set as it was configured at the end of the session
CVE	-----
Ease of Exploitation	Medium
Impact	An attacker can keep the session open for long by sending dumpy request for every minute
Recommendations	It is recommended to set an expiration of cookie to end the session after certain time frame.
Snapshot	 203.110.84.90/dop/admin/workbench/create Add content My Workbench Configuration Help My drafts Hello dopcreator MY CONTENT CREATE CONTENT MY D Acts Announcement Article Award Banner Basic page Circulars Division Branch Document Event FAQs Forms Minister News Parliament (Q & A) Photo Gallery Press Release Project / Programs / Initiative Publication Related links Schemes Services Slider Speeches/Interviews Tender Webcast Webform Whos who ensitive content like news, press releases or blog posts. ur static content, such as an 'About us' page. /Office orders/Gazette Notifications
Affected Site	http://203.110.84.90/dop/user/admin/workbench/create
Compliance Status	Not Complied

4) Vulnerability Title: Improper Captcha Implementation	
Risk	**Medium**
Abstract	It is observed that the user can login into the application without captcha.
CVE	-----
Ease of Exploitation	Medium
Impact	An attacker can brute force at input forms(with dummy data) which could lead to increase in logs or database entries on the server
Recommendations	It is recommended to review the captcha validation process and to make sure captcha validation is done before the user validation.
Snapshot	 404 Not Found User account | MINISTRY 203.110.84.90/dop/user About the Ministry+ Documents+ Parliament Q & A+ Notices+ Tenders Media+ RTI+ Home » User account Log in Forgot your password? 4:04 PM 09/03/2016 User account Username * wrongusername Enter your MINISTRY OF DEFENCE username. Password * •••••••••••••••••••••••••••• Enter the password that accompanies your username. CAPTCHA This question is for testing whether or not you are a human visitor and to prevent automated spam submissions. N 46 LT7 What code is in the image? * djaksdlaskjdas Enter the characters shown in the image. Wrong username Wrong password Wrong Captcha  404 Not Found User account | MINISTRY 203.110.84.90/dop/user About the Ministry+ Documents+ Parliament Q & A+ Notices+ Tenders Media+ RTI+ Home » User account Log in Forgot your password? Website Policies Help Contact us Feedback Disclaimer Visitor Analytics Select Language 4:06 PM 09/03/2016 User account Username * wrongusername Enter your MINISTRY OF DEFENCE username. Password * Enter the password that accompanies your username. Captcha Disappeared Website Content Managed by Ministry of Defence Designed, Developed and Hosted by National Informatics Centre(NIC) Last Updated: 09 Mar 2016

	
Affected Site	http://203.110.84.90/dop/user
Compliance Status	Not Complied

203.110.84.90/dop/user

Home » User account

User account

Username * dopcreator
Enter your MINISTRY OF DEFENCE username.

Password * ••••••••••••••
Enter the password that accompanies your username.

Log in

Forgot your password?

Correct Username
Correct Password

User can login
without Capthca

Website Content Managed by Ministry of Defence
Designed, Developed and Hosted by National Informatics Centre(NIC)
Last Updated: 09 Mar 2016

4:07 PM
09/03/2016

203.110.84.90/dop/admin/workbench

My Profile

dopcreator

My Edits

You haven't created or edited any content.

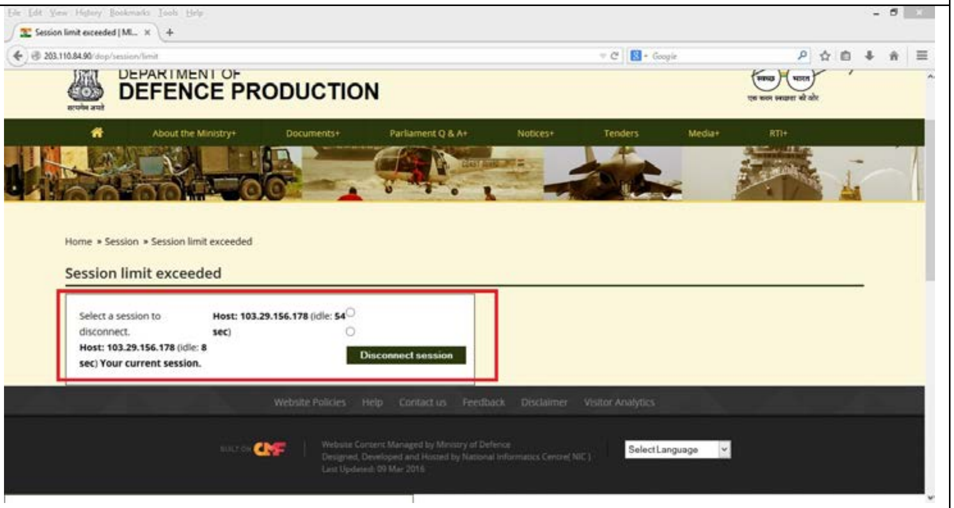
Login Successful Without Captcha

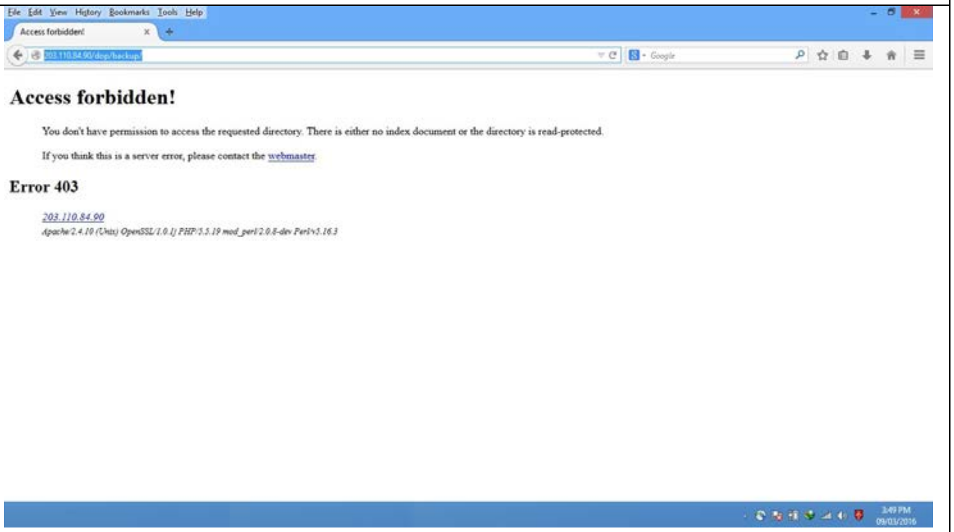
view all

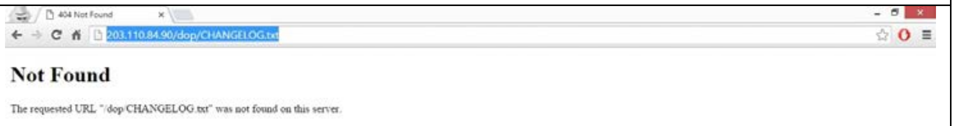
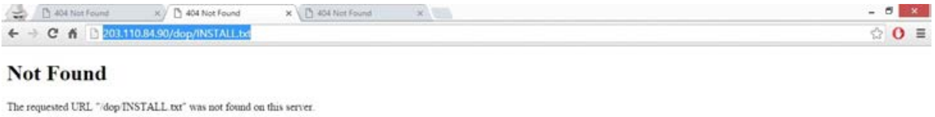
All Recent Content

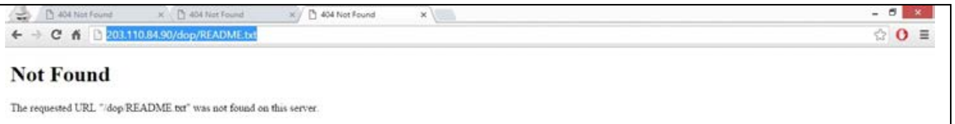
TITLE	TYPE	AUTHOR	LAST UPDATED	ACTIONS
Nodal Officers	side block	admin	4 hours 4 min ago	
Parliament Matters	side block	admin	4 hours 44 min ago	
Public Grievances CPGRAMs Portal	side block	admin	4 hours 45 min ago	
Vacancy & Circular	side block	admin	4 hours 47 min ago	
error	Article	admin	21 hours 33 min ago	
photo 4	Photo Gallery Home	admin	23 hours 4 min ago	
photo 3	Photo Gallery Home	admin	23 hours 5 min ago	
photo 2	Photo Gallery Home	admin	23 hours 7 min ago	
Image one	Photo Gallery Home	admin	23 hours 35 min ago	
Defence Exports		admin	1 day 33 min ago	

4:07 PM
09/03/2016

5) **Vulnerability Title: Multiple Browser Login**	
Risk	**Medium**
Abstract	It is observed that the same user can login into via multiple browsers.
CVE	-----
Ease of Exploitation	Medium
Impact	The attacker can use the same login ID for exploitation even if the ID is active.
Recommendations	It is recommended to restrict multiple browser login.
Snapshot	 203.110.84.90/dop/session/limit Home » Session » Session limit exceeded Session limit exceeded Select a session to disconnect. ○ Host: 103.29.156.178 (idle: 54 sec) ○ Host: 103.29.156.178 (idle: 8 sec) Your current session. Disconnect session Session limit exceeded | M... DEPARTMENT OF DEFENCE PRODUCTION About the Ministry+ Documents+ Parliament Q & A+ Notices+ Tenders Media+ RTI+ Website Policies Help Contact us Feedback Disclaimer Visitor Analytics Website Content Managed by Ministry of Defence Designed, Developed and Hosted by National Informatics Centre(NIC) Last Updated: 09 Mar 2016 Select Language
Affected Site	http://203.110.84.90/dop/user
Compliance Status	Complied

6) Vulnerability Title: Application Error	
Risk	**Low**
Abstract	It was observed that there was vital information leakage on website.
CVE	-----
Ease of Exploitation	Easy
Impact	It is possible to gather sensitive debugging information.
Recommendations	It is recommended to implement proper validations on all input fields of the web application and implement a customize error page.
Snapshot	 File Edit View History Bookmarks Tools Help Access forbidden! 203.110.84.90/dop/backup/ Google 3:49 PM 09/03/2016 **Access forbidden!** You don't have permission to access the requested directory. There is either no index document or the directory is read-protected. If you think this is a server error, please contact the webmaster. **Error 403** 203.110.84.90 Apache/2.4.10 (Unix) OpenSSL/1.0.1j PHP/5.5.19 mod_perl/2.0.8-dev Perl/v5.16.3
Affected Site	All Links
Compliance Status	Not Complied

7) Vulnerability Title: Drupal Default Documentation	
Risk	**Low**
Abstract	It was observed that Drupal default documentation was present on the application
CVE	-----
Ease of Exploitation	Easy
Impact	As per OWASP best practices the documentation must not be there in the web application
Recommendations	It is recommended to remove the documentation from the web application.
Snapshot	 **Not Found** The requested URL "/dop/CHANGELOG.txt" was not found on this server.  404 Not Found 404 Not Found 404 Not Found 203.110.84.90/dop/INSTALL.txt **Not Found** The requested URL "/dop/INSTALL.txt" was not found on this server.

	 404 Not Found 404 Not Found 404 Not Found 203.110.84.90/dop/README.txt **Not Found** The requested URL "/dop/README.txt" was not found on this server.
Affected Site	http://203.110.84.90/dop/CHANGELOG.txt http://203.110.84.90/dop/INSTALL.txt http://203.110.84.90/dop/README.txt
Compliance Status	Complied