CHIMERA CONSOLIDATED REPORT   
[https://eth.dapps.network](https://eth.dapps.network/)

The below report outlines vulnerability and informational findings that were discovered via automated scanning. It is possible that there are other vulnerabilities that were not discovered during automated scanning and are therefore not included on this report. You should always supplement automated scanning with manual security testing. It is also possible that some or all of these findings are false positives. All reported items should therefore be verified manually.

The attack vector and evidence of vulnerability associated with each item is listed with a description of the vulnerability. Suggested remediation steps and additional educational resources for each class of vulnerability are also provided.

Please note that this is not a comprehensive list of vulnerabilities in your application. Similiar and additional vulnerabilites outside of this report may exist. Please look through your entire codebase for additional security issues.

**Contents**

1. [SSL Configuration](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln1)
   1. [https://eth.dapps.network](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln1_1)
2. [Incomplete or No Cache-control and Pragma HTTP Header Set](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln2)
   1. [https://eth.dapps.network](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln2_1)
   2. [https://eth.dapps.network/robots.txt](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln2_2)
   3. [https://eth.dapps.network/sitemap.xml](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln2_3)
3. [Cookie set without secure flag](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln3)
   1. [https://eth.dapps.network](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln3_1)
   2. [https://eth.dapps.network/robots.txt](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln3_2)
   3. [https://eth.dapps.network/sitemap.xml](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_vuln3_3)
4. [Server Scan Results](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_serverscans)
   1. [Port Detection](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_portDetection)
   2. [Port 80](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_nikto80)
   3. [Port 443](https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=05e19debb2&view=att&th=15e15d61eb01ec03&attid=0.1&disp=inline&realattid=f_j6qvj5u40&safe=1&zw&saddbat=ANGjdJ-t8yQiy9k-1SIfG5iTe9t6_hRKidkdxs_sAQH8LXEfpY2XcJ7WWRoNe_sEKNfuKR0ed_YdnG5xr_d4cgJerZEHEcOeyCbajrNxhaf0dzM7e9MvDZ1m2T7-wkj73_m8-X5G2KmrDKxkag4imF7g0qnOZf5YHI2ku8G0eoRmns7etry7I9-tUlhWRTksqH_hcaRvGoOO_olk29SipRZnNMdXXYJSXE_Tr9DuxxDqZCyFWNGTlXCWOp4eDMG0RdM0kcO9seE2wIApS_pYuH6DsOVFaF4BOvRzsVBnGMnlqSPW5d6SphuoY9zxbZQeTKK_iY-0Iqd1zk8r2Ztu3Kc4bG7HQOvLMeKStd58ajZ23MnACOkqgcZw49WMHyFce7446pfk6Jhwva3BlgStRM0AI3MfxPnnEmtzb0JKbI5tquxNZ7QddKKa5TIGD0DL8JmYfgPrk_MqCPaOnzNvyNQ3N76_TG4GxU3xXtPJXNTmtQTpQI7L98zL8269bU46wW7GCHZN5B_QTGQ60Kcp8lwblbIWCN6qDKjQwjUO-YZdmn4eHcys544K0FpjwpBBJBWwH8uso0qHSZ1TFwAnLfBPH0s97jHz-Pj8aZS6wHxUJlbVu-E5XZLIyROuoVk#0.1_nikto443)

SSL Configuration

**Risk Level**

High

**Issue Description**

Due to historic export restrictions of high grade cryptography, legacy and new web servers are often able and configured to handle weak cryptographic options.

Even if high grade ciphers are normally used and installed, some server misconfiguration could be used to force the use of a weaker cipher to gain access to the supposed secure communication channel.

Ciphers such as SSLv2 should not be supported by the server, nor should ciphers that utilize a NULL cipher or have weak key lengths.

**Reference Links**

<https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)>

**CWE Reference**

[CWE-310](http://cwe.mitre.org/data/definitions/310.html)

**WASC Reference**

[WASC-14](http://projects.webappsec.org/Server-Misconfiguration)

**Remediation Steps**

Ensure that your server's SSL configuration utilizes a valid, trusted certificate and strong ciphers.

**Finding 1 of 1**

**URL**

[https://eth.dapps.network](https://eth.dapps.network/)

**Issues**

- SSL Certificate Issues

**Details**

[INFO] SSL Library Detected:

Certificate does not match server hostname

**Full Scan Results (Unparsed)**

SCAN RESULTS FOR ETH.DAPPS.NETWORK:443 - [13.65.243.110:443](http://13.65.243.110:443/)

----------------------------------------------------------

\* SSLV2 Cipher Suites:

Server rejected all cipher suites.

\* Session Resumption:

With Session IDs: Partially supported (1 successful, 4 failed, 0 errors, 5 total attempts). Try --resum\_rate.

With TLS Session Tickets: Not Supported - TLS ticket not assigned.

\* Session Renegotiation:

Client-initiated Renegotiations: Rejected

Secure Renegotiation: Supported

\* Compression:

DEFLATE Compression: Disabled

\* Heartbleed:

OpenSSL Heartbleed: NOT vulnerable

\* SSLV3 Cipher Suites:

Server rejected all cipher suites.

\* Certificate - Content:

SHA1 Fingerprint: e959fd5c80f76df7a593aae09686e604f74be8b0

Common Name: \*.[azurewebsites.net](http://azurewebsites.net/)

Issuer: {'countryName': 'US', 'localityName': 'Redmond', 'organizationalUnitName': 'Microsoft IT', 'organizationName': 'Microsoft Corporation', 'commonName': 'Microsoft IT SSL SHA2', 'stateOrProvinceName': 'Washington'}

Serial Number: 5A000498AF9A6412B7632517040001000498AF

Not Before: Sep 28 21:45:23 2016 GMT

Not After: May 7 17:03:30 2018 GMT

Signature Algorithm: sha256WithRSAEncryption

Key Size: 2048 bit

Exponent: 65537 (0x10001)

X509v3 Subject Alternative Name: {'DNS': ['\*.[azurewebsites.net](http://azurewebsites.net/)', '\*.[scm.azurewebsites.net](http://scm.azurewebsites.net/)', '\*.[azure-mobile.net](http://azure-mobile.net/)', '\*.[scm.azure-mobile.net](http://scm.azure-mobile.net/)']}

\* Certificate - Trust:

Hostname Validation: FAILED - Certificate does NOT match eth.dapps.network

"Mozilla NSS - 01/2014" CA Store: OK - Certificate is trusted

"Apple - OS X 10.9.2" CA Store: OK - Certificate is trusted

"Java 6 - Update 65" CA Store: OK - Certificate is trusted

"Microsoft - 04/2014" CA Store: OK - Certificate is trusted

\* Certificate - OCSP Stapling:

OCSP Response Status: successful

Validation w/ Mozilla's CA Store: Response is Trusted

Responder Id: FFE1DC933CD37C3716D115404E3670DB49FF657C

Cert Status: good

Cert Serial Number: 5A000498AF9A6412B7632517040001000498AF

This Update: Aug 23 02:55:08 2017 GMT

Next Update: Aug 27 02:55:08 2017 GMT

\* TLSV1\_2 Cipher Suites:

Preferred:

ECDHE-RSA-AES256-SHA384 256 bits HTTP 200 OK

Accepted:

ECDHE-RSA-AES256-SHA384 256 bits HTTP 200 OK

ECDHE-RSA-AES256-SHA 256 bits HTTP 200 OK

AES256-SHA256 256 bits HTTP 200 OK

AES256-SHA 256 bits HTTP 200 OK

AES256-GCM-SHA384 256 bits HTTP 200 OK

ECDHE-RSA-AES128-SHA256 128 bits HTTP 200 OK

ECDHE-RSA-AES128-SHA 128 bits HTTP 200 OK

AES128-SHA256 128 bits HTTP 200 OK

AES128-SHA 128 bits HTTP 200 OK

AES128-GCM-SHA256 128 bits HTTP 200 OK

\* TLSV1\_1 Cipher Suites:

Preferred:

ECDHE-RSA-AES256-SHA 256 bits HTTP 200 OK

Accepted:

ECDHE-RSA-AES256-SHA 256 bits HTTP 200 OK

AES256-SHA 256 bits HTTP 200 OK

ECDHE-RSA-AES128-SHA 128 bits HTTP 200 OK

AES128-SHA 128 bits HTTP 200 OK

\* TLSV1 Cipher Suites:

Preferred:

ECDHE-RSA-AES256-SHA 256 bits Server response was not HTTP

Accepted:

ECDHE-RSA-AES256-SHA 256 bits Server response was not HTTP

AES256-SHA 256 bits Server response was not HTTP

ECDHE-RSA-AES128-SHA 128 bits Server response was not HTTP

AES128-SHA 128 bits Server response was not HTTP

Incomplete or No Cache-control and Pragma HTTP Header Set

**Risk Level**

Low

**Issue Description**

The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.

**Reference Links**

<https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching>

**CWE Reference**

[CWE-525](http://cwe.mitre.org/data/definitions/525.html)

**Remediation Steps**

Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate, private; and that the pragma HTTP header is set with no-cache.

**Finding 1 of 3**

**URL**

[https://eth.dapps.network](https://eth.dapps.network/)

**Request**

GET [https://eth.dapps.network](https://eth.dapps.network/) HTTP/1.0

User-Agent: Python-urllib/1.17

Host: eth.dapps.network

**Response**

HTTP/1.1 200 OK

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Content-Length: 24

Content-Type: text/html; charset=utf-8

Expires: 0

ETag: W/"18-MLjPamvIGD6CfWN1AXqLg2rHK+k"

Server: Microsoft-IIS/8.0

Surrogate-Control: no-store

X-Content-Type-Options: nosniff

Expect-CT: max-age=2592000

Referrer-Policy: no-referrer

Content-Security-Policy: default-src 'self'; style-src 'self'

X-Content-Security-Policy: default-src 'self'; style-src 'self'

X-WebKit-CSP: default-src 'self'; style-src 'self'

X-Frame-Options: SAMEORIGIN

X-DNS-Prefetch-Control: off

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-XSS-Protection: 1; mode=block

Access-Control-Allow-Origin: \*

Access-Control-Allow-Methods: PUT,POST,DELETE

Access-Control-Allow-Headers: Content-Type, Authorization,Accept

X-Powered-By: [ASP.NET](http://asp.net/)

Set-Cookie: ARRAffinity=341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

Date: Thu, 24 Aug 2017 19:08:50 GMT

Connection: close

Welcome to Dapps Network

**Finding 2 of 3**

**URL**

<https://eth.dapps.network/robots.txt>

**Request**

GET <https://eth.dapps.network/robots.txt> HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0

Pragma: no-cache

Cache-Control: no-cache

Content-Length: 0

Host: eth.dapps.network

**Response**

HTTP/1.1 404 Not Found

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Content-Length: 149

Content-Type: text/html; charset=utf-8

Expires: 0

Server: Microsoft-IIS/8.0

Surrogate-Control: no-store

X-Content-Type-Options: nosniff

Expect-CT: max-age=2592000

Referrer-Policy: no-referrer

Content-Security-Policy: default-src 'self'

X-Frame-Options: SAMEORIGIN

X-DNS-Prefetch-Control: off

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-XSS-Protection: 1; mode=block

Access-Control-Allow-Origin: \*

Access-Control-Allow-Methods: PUT,POST,DELETE

Access-Control-Allow-Headers: Content-Type, Authorization,Accept

X-Powered-By: [ASP.NET](http://asp.net/)

Set-Cookie: ARRAffinity=341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

Date: Thu, 24 Aug 2017 19:08:57 GMT

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Error</title>

</head>

<body>

<pre>Cannot GET /robots.txt</pre>

</body>

</html>

**Finding 3 of 3**

**URL**

<https://eth.dapps.network/sitemap.xml>

**Request**

GET <https://eth.dapps.network/sitemap.xml> HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0

Pragma: no-cache

Cache-Control: no-cache

Content-Length: 0

Host: eth.dapps.network

**Response**

HTTP/1.1 404 Not Found

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Content-Length: 150

Content-Type: text/html; charset=utf-8

Expires: 0

Server: Microsoft-IIS/8.0

Surrogate-Control: no-store

X-Content-Type-Options: nosniff

Expect-CT: max-age=2592000

Referrer-Policy: no-referrer

Content-Security-Policy: default-src 'self'

X-Frame-Options: SAMEORIGIN

X-DNS-Prefetch-Control: off

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-XSS-Protection: 1; mode=block

Access-Control-Allow-Origin: \*

Access-Control-Allow-Methods: PUT,POST,DELETE

Access-Control-Allow-Headers: Content-Type, Authorization,Accept

X-Powered-By: [ASP.NET](http://asp.net/)

Set-Cookie: ARRAffinity=341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

Date: Thu, 24 Aug 2017 19:08:56 GMT

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Error</title>

</head>

<body>

<pre>Cannot GET /sitemap.xml</pre>

</body>

</html>

Cookie set without secure flag

**Risk Level**

Low

**Issue Description**

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

**Reference Links**

<http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)>

**CWE Reference**

[CWE-614](http://cwe.mitre.org/data/definitions/614.html)

**WASC Reference**

[WASC-13](http://projects.webappsec.org/Information-Leakage)

**Remediation Steps**

Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted tunnel. Ensure that the secure flag is set for cookies containing such sensitive information.

**Finding 1 of 3**

**URL**

[https://eth.dapps.network](https://eth.dapps.network/)

**Attack**

341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

**Parameter**

ARRAffinity

**Request**

GET [https://eth.dapps.network](https://eth.dapps.network/) HTTP/1.0

User-Agent: Python-urllib/1.17

Host: eth.dapps.network

**Response**

HTTP/1.1 200 OK

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Content-Length: 24

Content-Type: text/html; charset=utf-8

Expires: 0

ETag: W/"18-MLjPamvIGD6CfWN1AXqLg2rHK+k"

Server: Microsoft-IIS/8.0

Surrogate-Control: no-store

X-Content-Type-Options: nosniff

Expect-CT: max-age=2592000

Referrer-Policy: no-referrer

Content-Security-Policy: default-src 'self'; style-src 'self'

X-Content-Security-Policy: default-src 'self'; style-src 'self'

X-WebKit-CSP: default-src 'self'; style-src 'self'

X-Frame-Options: SAMEORIGIN

X-DNS-Prefetch-Control: off

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-XSS-Protection: 1; mode=block

Access-Control-Allow-Origin: \*

Access-Control-Allow-Methods: PUT,POST,DELETE

Access-Control-Allow-Headers: Content-Type, Authorization,Accept

X-Powered-By: [ASP.NET](http://asp.net/)

Set-Cookie: ARRAffinity=341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

Date: Thu, 24 Aug 2017 19:08:50 GMT

Connection: close

Welcome to Dapps Network

**Finding 2 of 3**

**URL**

<https://eth.dapps.network/robots.txt>

**Attack**

341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

**Parameter**

ARRAffinity

**Request**

GET <https://eth.dapps.network/robots.txt> HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0

Pragma: no-cache

Cache-Control: no-cache

Content-Length: 0

Host: eth.dapps.network

**Response**

HTTP/1.1 404 Not Found

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Content-Length: 149

Content-Type: text/html; charset=utf-8

Expires: 0

Server: Microsoft-IIS/8.0

Surrogate-Control: no-store

X-Content-Type-Options: nosniff

Expect-CT: max-age=2592000

Referrer-Policy: no-referrer

Content-Security-Policy: default-src 'self'

X-Frame-Options: SAMEORIGIN

X-DNS-Prefetch-Control: off

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-XSS-Protection: 1; mode=block

Access-Control-Allow-Origin: \*

Access-Control-Allow-Methods: PUT,POST,DELETE

Access-Control-Allow-Headers: Content-Type, Authorization,Accept

X-Powered-By: [ASP.NET](http://asp.net/)

Set-Cookie: ARRAffinity=341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

Date: Thu, 24 Aug 2017 19:08:57 GMT

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Error</title>

</head>

<body>

<pre>Cannot GET /robots.txt</pre>

</body>

</html>

**Finding 3 of 3**

**URL**

<https://eth.dapps.network/sitemap.xml>

**Attack**

341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

**Parameter**

ARRAffinity

**Request**

GET <https://eth.dapps.network/sitemap.xml> HTTP/1.1

User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0

Pragma: no-cache

Cache-Control: no-cache

Content-Length: 0

Host: eth.dapps.network

**Response**

HTTP/1.1 404 Not Found

Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate

Pragma: no-cache

Content-Length: 150

Content-Type: text/html; charset=utf-8

Expires: 0

Server: Microsoft-IIS/8.0

Surrogate-Control: no-store

X-Content-Type-Options: nosniff

Expect-CT: max-age=2592000

Referrer-Policy: no-referrer

Content-Security-Policy: default-src 'self'

X-Frame-Options: SAMEORIGIN

X-DNS-Prefetch-Control: off

Strict-Transport-Security: max-age=15552000; includeSubDomains

X-Download-Options: noopen

X-XSS-Protection: 1; mode=block

Access-Control-Allow-Origin: \*

Access-Control-Allow-Methods: PUT,POST,DELETE

Access-Control-Allow-Headers: Content-Type, Authorization,Accept

X-Powered-By: [ASP.NET](http://asp.net/)

Set-Cookie: ARRAffinity=341b768fc49455e18091f5063d13391e034e3b8570558d994fba7687534feb33;Path=/;HttpOnly;Domain=eth.dapps.network

Date: Thu, 24 Aug 2017 19:08:56 GMT

<!DOCTYPE html>

<html lang="en">

<head>

<meta charset="utf-8">

<title>Error</title>

</head>

<body>

<pre>Cannot GET /sitemap.xml</pre>

</body>

</html>

Server Scans

**Issue Description**

Scans are run against active ports on your server using [Nikto](https://cirt.net/nikto2" \t "_blank), which tests for potentially dangerous files/programs, outdated versions of server software, and version specific problems. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

Not every check is a security problem, though most are. There are some items that are "info only" type checks that look for things that may not have a security flaw, but the webmaster or security engineer may not know are present on the server. These items are usually marked appropriately in the information printed. There are also some checks for unknown items which have been seen scanned for in log files.

Ports 80 and 443 are scanned by default. Any other ports that were scanned were scanned because they were detected as open on your server through running an [nmap](http://nmap.org/" \t "_blank) scan.

**Risk Level**

**Informational / Other**

These scans are run against your server to provide you with additional information about your application and server's attack surface. The presence of these scan results does not inherently represent a vulnerability, but they should be carefully analyzed.

**Reference Links**

<http://nmap.org/>  
  
<https://cirt.net/nikto2>

**Port Detection**

**Detection Results**

Port 80 (tcp) - open based on syn-ack detection, running 'http' service

Port 443 (tcp) - open based on syn-ack detection, running 'https' service

**Port 80**

**Scan Details**

- Nikto v2.1.5

---------------------------------------------------------------------------

+ Target IP: 13.65.243.110

+ Target Hostname: eth.dapps.network

+ Target Port: 80

+ Start Time: 2017-08-24 19:09:42 (GMT0)

---------------------------------------------------------------------------

+ Server: Microsoft-IIS/8.0

+ Retrieved x-powered-by header: [ASP.NET](http://asp.net/)

+ Server leaks inodes via ETags, header found with file /, fields: 0xW/18 0xMLjPamvIGD6CfWN1AXqLg2rHK+k

+ Uncommon header 'x-webkit-csp' found, with contents: default-src 'self'; style-src 'self'

+ Uncommon header 'access-control-allow-origin' found, with contents: \*

+ Uncommon header 'content-security-policy' found, with contents: default-src 'self'; style-src 'self'

+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block

+ Uncommon header 'access-control-allow-headers' found, with contents: Content-Type, Authorization,Accept

+ Uncommon header 'expect-ct' found, with contents: max-age=2592000

+ Uncommon header 'x-content-security-policy' found, with contents: default-src 'self'; style-src 'self'

+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN

+ Uncommon header 'referrer-policy' found, with contents: no-referrer

+ Uncommon header 'x-dns-prefetch-control' found, with contents: off

+ Uncommon header 'access-control-allow-methods' found, with contents: PUT,POST,DELETE

+ Uncommon header 'surrogate-control' found, with contents: no-store

+ Uncommon header 'strict-transport-security' found, with contents: max-age=15552000; includeSubDomains

+ Uncommon header 'x-content-type-options' found, with contents: nosniff

+ Uncommon header 'x-download-options' found, with contents: noopen

+ Cookie ARRAffinity created without the httponly flag

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Server banner has changed from 'Microsoft-IIS/8.0' to 'Microsoft-HTTPAPI/2.0' which may suggest a WAF, load balancer or proxy is in place

+ Allowed HTTP Methods: GET, HEAD

+ DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx> for details.

+ Retrieved x-aspnet-version header: 4.0.30319

+ 6544 items checked: 0 error(s) and 21 item(s) reported on remote host

+ End Time: 2017-08-24 19:14:52 (GMT0) (310 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

**Port 443**

**Scan Details**

- Nikto v2.1.5

---------------------------------------------------------------------------

+ Target IP: 13.65.243.110

+ Target Hostname: eth.dapps.network

+ Target Port: 443

---------------------------------------------------------------------------

+ SSL Info: Subject: /CN=\*.[azurewebsites.net](http://azurewebsites.net/)

Ciphers: ECDHE-RSA-AES256-SHA384

Issuer: /C=US/ST=Washington/L=Redmond/O=Microsoft Corporation/OU=Microsoft IT/CN=Microsoft IT SSL SHA2

+ Start Time: 2017-08-24 19:14:54 (GMT0)

---------------------------------------------------------------------------

+ Server: Microsoft-IIS/8.0

+ Retrieved x-powered-by header: [ASP.NET](http://asp.net/)

+ Server leaks inodes via ETags, header found with file /, fields: 0xW/18 0xMLjPamvIGD6CfWN1AXqLg2rHK+k

+ Uncommon header 'referrer-policy' found, with contents: no-referrer

+ Uncommon header 'access-control-allow-headers' found, with contents: Content-Type, Authorization,Accept

+ Uncommon header 'x-frame-options' found, with contents: SAMEORIGIN

+ Uncommon header 'x-xss-protection' found, with contents: 1; mode=block

+ Uncommon header 'expect-ct' found, with contents: max-age=2592000

+ Uncommon header 'x-dns-prefetch-control' found, with contents: off

+ Uncommon header 'x-content-security-policy' found, with contents: default-src 'self'; style-src 'self'

+ Uncommon header 'x-content-type-options' found, with contents: nosniff

+ Uncommon header 'surrogate-control' found, with contents: no-store

+ Uncommon header 'access-control-allow-origin' found, with contents: \*

+ Uncommon header 'content-security-policy' found, with contents: default-src 'self'; style-src 'self'

+ Uncommon header 'x-webkit-csp' found, with contents: default-src 'self'; style-src 'self'

+ Uncommon header 'access-control-allow-methods' found, with contents: PUT,POST,DELETE

+ Uncommon header 'strict-transport-security' found, with contents: max-age=15552000; includeSubDomains

+ Uncommon header 'x-download-options' found, with contents: noopen

+ Cookie ARRAffinity created without the secure flag

+ Cookie ARRAffinity created without the httponly flag

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Server banner has changed from 'Microsoft-IIS/8.0' to 'Microsoft-HTTPAPI/2.0' which may suggest a WAF, load balancer or proxy is in place

+ Server is using a wildcard certificate: '\*.[azurewebsites.net](http://azurewebsites.net/)'

+ Hostname 'eth.dapps.network' does not match certificate's CN '\*.[azurewebsites.net](http://azurewebsites.net/)'

+ Allowed HTTP Methods: GET, HEAD

+ DEBUG HTTP verb may show server debugging information. See <http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx> for details.

+ Retrieved x-aspnet-version header: 4.0.30319

+ 6544 items checked: 0 error(s) and 24 item(s) reported on remote host

+ End Time: 2017-08-24 19:32:32 (GMT0) (1058 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested

Report provided by Salesforce Product Security and does not represent in any way a guarantee of security   
  
Information contained in this report may be confidential   
  
Generated 08/24/2017 at 07:33 PM GMT   
  
Report ID 89c16231-79a0-4ecc-8586-4120e2713a39 - please reference in any communication regarding this report