1 PAGE REPORT

EXPLOITATION OF CONTENT MANAGEMENT SYSTEM TO LAUNCH LARGE SCALE CYBER-ATTACKS

MANOJ KUMAR SWAMI(VTU4573)
ANKIT PANDEY(VTU4131)

Company Logo & Name: CERT-In, New Delhi Department of Computer Science and Engineering

Internal Guide: R. Vinoth Kumar

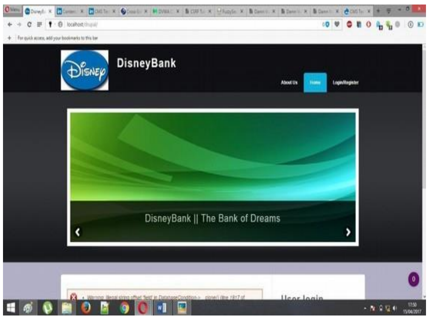
Objective/Motivation:

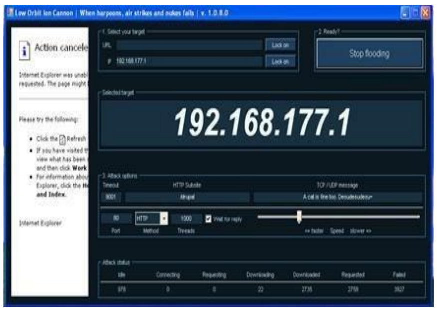
Content Management Systems are mostly used for website development. Websites are the main targets of various malicious attackers, and therefore it is necessary to be knowledge about the security level of websites. This will describe some features of the well-known open source Content Management System platforms: Drupal, WordPress and Joomla. The security of such web applications depends as much on vulnerabilities found in plugins as it does in vulnerabilities in the application core. One of the biggest problems facing the IT security industry is the use of vulnerabilities in legitimate software to launch malware attacks. Malicious programs can use these vulnerabilities to infect a Content of Websites without attracting the attention of the user and in some cases, without triggering an alert from security software.

Results:

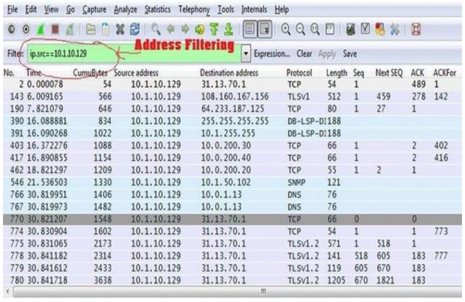
In this project, basic features of CMSs have been presented. Critical web vulnerabilities against web applications have been explained. Each vulnerability has been tested on the basic installation of the tested CMSs (Drupal) and possible security measures have been listed. The test results of the CMS systems have been presented as well as the list of threats against which the tested CMS systems were resistant in their basic installations. Based on findings the vulnerabilities we can conclude that servers, web servers and database servers used to host most popular CMS explained in project are not less secure than those used to host other CMS if proposed alternatives are used.

Keywords: Drupal, LOIC(Dos Tool), Wireshark.





Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Address Filtering
Expression... Clear Apply Save

Filter: ip.src==10.1.10.129

No.	Time	CumuBytes	Source address	Destination address	Protocol	Length	Seq	Next SEQ	ACK	ACKFor
2	0.000078	54	10.1.10.129	31.13.70.1	TCP	54	1		489	1
143	6.009165	566	10.1.10.129	108.160.167.156	TLSv1	512	1	459	278	142
190	7.821079	646	10.1.10.129	64.233.187.125	TCP	80	1	27	1	
390	16.088881	834	10.1.10.129	255.255.255.255	DB-LSP-DI	188				
391	16.090268	1022	10.1.10.129	10.1.255.255	DB-LSP-DI	188				
403	16.372276	1088	10.1.10.129	10.0.200.30	TCP	66	1		2	402
417	16.890855	1154	10.1.10.129	10.0.200.40	TCP	66	1		2	416
462	18.821297	1209	10.1.10.129	10.0.200.20	TCP	55	1	2	1	
546	21.536503	1330	10.1.10.129	10.1.50.102	SNMP	121				
766	30.819951	1406	10.1.10.129	10.0.1.13	DNS	76				
767	30.819973	1482	10.1.10.129	10.0.1.13	DNS	76				
770	30.821207	1548	10.1.10.129	31.13.70.1	TCP	66	0		0	
774	30.830904	1602	10.1.10.129	31.13.70.1	TCP	54	1		1	773
775	30.831065	2173	10.1.10.129	31.13.70.1	TLSv1.2	571	1	518	1	
778	30.841182	2314	10.1.10.129	31.13.70.1	TLSv1.2	141	518	605	183	777
779	30.841612	2433	10.1.10.129	31.13.70.1	TLSv1.2	119	605	670	183	
780	30.841718	3638	10.1.10.129	31.13.70.1	TLSv1.2	1205	670	1821	183	

Email Id: manojswami600@gmail.com, ankitpandey035@gmail.com

YouTube Link: https://www.youtube.com/watch?v=6TBmHLzOjIY

Project Details 2016 – 2017

1. **Batch No** : 29
2. **College Name** : Veltech Dr. RR & Dr. SR University
3. **Department** : Computer Science and Engineering
4. **Project Title** : Exploitation of Content Management System Vulnerabilities to launch Large Scale Cyber-Attacks
5. **Student Name, MOB No with E Mail ID (All Batch Mates):**

S.no.	Name	Mobile No.	E-Mail ID
1	Manoj Kumar Swami	+91 7845803074	manojswami600@gmail.com
2	Ankit Pandey	+91 9884077798	ankitpandey035@gmail.com

6. **Project Domain/ Area** : Cyber Security
7. **Project Cost** : Nil
8. **Company Name** : CERT-In
9. **Internal Guide /Mob No** : R. Vinoth Kumar / 9655262691
10. **External Guide/ Mob No** : Sh. Noorul Ameen A (Scientist-C)/ 011-2436855
11. **Project Kit/ Simulation** : Simulation
12. **Date Of submission** : 24/04/2017