



# INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

#### DEVELOPING A SECURE WORDPRESS WEBSITE AND HOSTING ON NIC PLATFORM

**Rohit Kumar**\*

Assistant Engineer, Uttarakhand Council for Biotechnology, Haldi-263146, Pantnagar, U. S. Nagar, Uttarakhand, India

#### DOI: 10.5281/zenodo.60877

#### ABSTRACT

Now-a-days most people explores the web at the end of the when a majority of business are closed and the reason being that websites are always there. A website allows us to do business for 24 hours a day, 7 days a week, 365 days a year. If your competitor has a website then they will have a definite advantage to influence your business or even if you have an informative website then also it will help you to make your stakeholders aware about the progress of your organization. Moreover with powerful search engines it is easier to locate your organization online. A professional website improves your public image and your customers/stakeholders will have more confidence in your organization. Most small businesses are only able to market to their town and surrounding communities. With a website, you can take your products and services globally.

With the edges of having a website it is required to develop a website but to develop a website it is an obvious thought that the knowledge of HTML, CSS, PHP, MYSQL, etc. is a must. This is not a necessity to have absolute knowledge of above languages although it is advantageous if you possess that, the reason being the availability of several open source content management system in the public domain some of them are wordpress, joomla and drupal. The basic knowledge of above CMS will help you developing websites in minute or hours.[1][2]

Now the other side of website development emphasizes the security constraint or the recovery after hack which is the common issues now-a-days with daily advancements in web technologies. Although there is a lot of online support for these abrupt issues but still a smart knowledge is required to deal with these issues to have a healthy website.

In the proposed work, the limitation associated with the website are studied and removed. The complete method was presented that how the website got secured after vulnerability detection.

**KEYWORDS:** wordpress, hack, security threat, website.

#### **INTRODUCTION**

In the past years, several days were required for the development of a professional website and a professional web developer team or expert was required for the same. But now the technological advancement brought us with several open source content management software platform such as wordpress, joomla and drupal eliminating the issue of the requirement of professional knowledge of website development but only some basic knowledge will drive us to create a professional website. Wordpress is considered in this paper as the work of the author http://www.ucb.uk.gov.in is in wordpress only. Firstly the security assessment report have been elaborated in this paper and thereafter the details of bugs fixation and verification have been described.[2]



## ISSN: 2277-9655 Impact Factor: 4.116

WordPress is a free and open-source content management system (CMS) written in PHP and based on MySQL licensed under the GPL.To create a website using wordpress the wordpress is installed on a web server. The basic features of wordpress includes a plugin architecture and a template system. Recently wordpress have been used by more than 26.4% in top 10 million websites. Being the easiest, wordpress is very popular blogging system on the Web. WordPress allows users to create and edit websites from a central control panel, which includes a text editor for modifying content and menus to change various design elements. WordPress provides various plugins in WordPress Plugin Directory, and it is quite easy to upload and promote plugins in WordPress. Users can write posts in this platform and other people can write comments about the post.[3]

WordPress has a web template system using a template processor having files size of about 20 MB. WordPress users can use different themes which allows to change the look and functionality of the website. The plugin architecture allows users to extend the features and functionality of a website or blog. WordPress also features integrated link management; a search engine–friendly, clean permalink structure; the ability to assign multiple categories to articles; and support for tagging of posts and articles. WordPress Multisites allows multiple blogs to exist within one installation but is able to be administered by a centralized maintainer.[3]

#### PROBLEM FORMULATION AND OBJECTIVES

In the past, millions of user implemented their website using wordpress. We also implemented our website <u>http://www.ucb.uk.gov.in</u> using wordpress open source content management system. In this work, we have implemented the website including security measures after vulnerability detection. In this first method, we will focus upon the level 1 vulnerability report including OWASP, SANS/CWE, WASC vulnerability standards[4]. In the second method we will include the ways to remove existing vulnerability. In this third method, we will check the website performance after the vulnerability patch-up.

Objectives for this work are:

- 1. To implement a website using wordpress custom design.
- 2. The main focus of this research is the detection of vulnerabilities to reduce the problem of hacking.
- 3. The objects of interest is testing on security platform.
- 4. To analyze the use of several plugin in performance enhancement.
- 5. To detect the recovery and security performance after hack.

## **RESEARCH METHODOLOGY**

The basic idea of secure designing of wordpress 4.2 is to create a website bugs free, then to update the website as soon as new bugs are reported. Till this work was completed now the wordpress have been updated to the version 4.5.2 which had fixed most of the reported issues.

In this research, we have followed the given steps to implement the research problem.

Step1: First we developed the website using wordpress 4.2.

Step2: Secondly we had undergone level 1 security audit to determine the vulnerabilities.

Step3: Then we implemented the required changes as per the fixation of the bugs.

Step4: Thereafter we have level 2 security assessment to determine if any vulnerability persists.

Step5: Finally, the website got hosted on  $\underline{http://www.ucb.uk.gov.in}$ .

Step6: Recent verification from online malware detecting softwares.

**3.1 Security Audit Level 1 report:** The website with wordpress 4.2 has following vulnerabilities according to the NIC website security audit vendor's report:



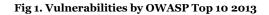
ISSN: 2277-9655 Impact Factor: 4.116

#### Table 1: Details of initial security audit report

Vulnerability Name	Severity	Status
Improper Session Termination	High	×
Stored Cross-Site Scripting	High	×
Session Fixation	High	×
File Upload Vulnerability	High	×
HTML Injection	High	X
Iframe Injection	High	X
Insufficient Transport Layer Protection(SSL/TLS)	Medium	×
Improper Cache Control	Medium	×
Login Brute Force	Medium	
Cookie Secure Attribute Not Present	Low	×
Auto-Complete Feature Enabled	Low	X
HTTPOnly Attribute Not Present	Low	×
Weak Password Policy	Low	X
Http Method Enabled	Low	X







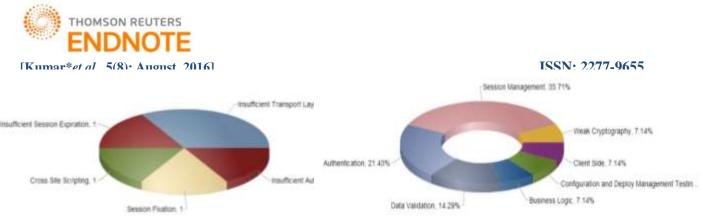


Fig 3. Vulnerabilities by SANS/CWE Top 25

Fig 4. Vulnerabilities by Category

#### **Vulnerability Details with Evidences**

**1. Improper Session Termination:** Improper session termination is a vulnerability which relates to the session management module of the application. The applications vulnerable to the improper session termination, do not properly terminate the application session due to which the authenticated pages in the application can later be browsed by pressing the browser's back button.[5]

A CONTRACTOR OF THE	and the second second		and the same	
			New York	
		and the second second		
	en Lanaras El constantes	-		
	Annual Street and Annual Street		WIN ALCO DUTING	-
			States and the second s	

Fig 5. Improper session termination vulnerability

**2. Stored Cross-Site Scripting**: A stored XSS attack occurs when a web application gathers a malicious input from user and stores the malicious input inside the vulnerable webpage permanently. Thus, this malicious code will be executed every time a user visits the vulnerable webpage. The input that is stored is not correctly filtered. As a consequence, the malicious data will appear to be part of the web site and run within the users browser under the privileges of the web application. For example: 1. Application offers a form to users to post their questions about the application and give feedback. 2. In social networking application, where a user can see other user((s profiles. 3. Comment form in application where user can post their comments.[6]



ISSN: 2277-9655 Impact Factor: 4.116

nk: http://incalficiel/ucli.uk.gov Media	maert Sildeshaw   Add Registratio	an Parm	Visuali Teet	Screent Options - Publish Saras Draft * Status: Draft <u>Eds</u> & Status: Draft <u>Eds</u> M Public <u>Draft Eds</u> Move to Trast	Prestaw
ng For XSS "> <svg <br="">nk: http://docafront/actual.gov Media 🔮 Genetia 🔳 i Int boquese aid int</svg>	undebout-us: VeerPeer	an Parm		Save Draft <sup>1</sup> Status: Draft <u>Edit</u> <sup>2</sup> Visibility: Public <u>Edit</u> <sup>2</sup> Publich immediately <u>E</u>	
nik http://focalitent/uch.uk.gov Media 🔛 Greenita 📰 a link bripanie del irro	undebout-us: VeerPeer	an Parm		Save Draft <sup>1</sup> Status: Draft <u>Edit</u> <sup>2</sup> Visibility: Public <u>Edit</u> <sup>2</sup> Publich immediately <u>E</u>	
Mostila 🛛 🏠 Germetita 🗍 🏧 b	maert Sildeshaw   Add Registratio			<ul> <li>Status: Draft <u>Sola</u></li> <li>Visibility: Public <u>Edit</u></li> <li>Publich immediately <u>So</u></li> </ul>	
Intel Series and I pro-	ing ut ut a sode m			<ul> <li>Wishifty: Public Edit</li> <li>Publich immediately Eg</li> </ul>	la -
					15
				Manager and Manager	
				Move to Trash	TROBILIN!
				Format	
				<ul> <li>Atide</li> </ul>	
				O J Audio	
				O THE Chat	
				C Sallary	
preview- true	Add New Poll - Ottavachand C. ×			\$ th + #	41 - 31
us- 📰 images- 🕥 Information-	🗧 Miscelaneous- 🧨 Outline- 🥜 R	esize- 🔀 Taoli- 🗰 View Source- 近 Optic	0.06-		- 1
	a service and	utal mat up	ting of	-	
				NO THE STATE	
	CONTRACTOR OF THE				
		2038/			
		OK	New		
4		ols Halp Add New Post - Utravisioned C × sprease-base me- Margae- Chlomation- Microtaneous- / Cultive- / Re	oli Halp Add Hen Port - Utransfrand C x / ) testing for XXX - j Utransfr x sprenze-stor me: I transfer I Moretaneous- / Outline / Restar X Tools II Vera Koncer II Opti CONTRACTOR INCOMENTS - Moretaneous- / Outline / Restar X Tools II Vera Koncer II Opti CONTRACTOR INCOMENTS - Outline / Restar X Tools II Vera Koncer II Opti CONTRACTOR INCOMENTS - Outline / Restar X Tools II Vera Koncer II Opti CONTRACTOR INCOMENTS - Outline / Restar X Tools II Vera Koncer II Opti CONTRACTOR INCOMENTS - Outline / Restar X Tools II Vera Koncer II Opti CONTRACTOR INCOMENTS - OUTLINE - OUTLIN	oli ±liip Add Nes-Port - Utrantitued C × () testing for XXX - (Utrantit × ) + testing for XXX - (Utrantit × ) + Utrantitue () + (Utrantitue () + (U	anti A este Lidep Add Here Port - Utransforman C (retring for XSS - ) (Muneik

Fig 6. Cross site scripting vulnerability

**3. Session Fixation:** Session fixation vulnerability occurs when the web application utilizes the preset session identifier instead of generating a new session identifier for every logon event. Application is also vulnerable to session fixation if the session ID issued at the login page is renewed on the successful login. An attacker can force a victim to use preset session identifier and gain access to victim's account once the session token is associated with the account.[7][8]

The example below explains the session fixation attack process:

1. The attacker establishes a legitimate connection with the web server to acquire a session ID or creates a new session with the proposed session ID.

2. Attacker then sends the crafted link with the established session ID to the victim.

3. Victim clicks the link sent by the attacker.

4. The web application renews the session ID instead of generating the new session ID.

5. On a successful login to the web application, the session ID gets activated and attacker then hijacks the victim's session.[7][8]



ISSN: 2277-9655 Impact Factor: 4.116

	Uttaral	hand Gouncil for Rister	× 1 +					
Iocalhost/arth.id.ans.in/our-Ingin)	andshattan			- C	in.		· · · · ·	
and the second se	nt- 🔛 imaget: 🕢 information- 🧱 Mate	dlaneous- 🥖 Dutine- 🥜	Reuze- X Took-					
			11000					
			100					
			No. and					
			Second Second					
		You are now for	and the state of t					
		CON MAR LIDEA 103	Step our.					
		Username						
		testin						
		ce sent						
		Pasiayord						
🗑 K > XX Consele HTM	L CSS Series DOM Net Cookies	-				PSearch within Contract	ponet	A
Cookies + Tilter + Default (Act								
Bame	Value	Domain	Raw Size	Fuilt		Expires	IttpOnly	* Security
# PHPSESS2D # wp-writings-2	+ 4 History 20 Junio Transmith	lacafreet lacafreet	20.0	Auth-uk.g	nicital.	12/04/2016 12:55: 10 pm		
iii wp-settings-time-2	1420000038	locafront.	28.8	Justs-uk-g	asc.any	12/04/2016 12:55: 50 pm		
# wordpress_test_cookie	were schoolse chemite.	locafhoait	36.6	Asto ukig	auc.int/	Gesport		
							41	a i Dia Dia Mil 19-24-3 - 8
	S Universal Cross Site Scripti	und - Uttankhasd Court	×\+					- 8
Create a new fiddle - /SFid × 1	Universal Cross Site Scription      Depthin				the first of the	ครูวิเริงอีกวิกมากามปรีว	9 • \$ \$ \$	
Create a new fiddle - ISFid = 1 file tocalhost with diagenerity able- 1 Cookles- CSS- 1 For	S Universal Cross Site Scripti				the first of the	eg Nato Trummurts	* \$ \$ \$	
Create a new fiddle - /SFid × 1	S Universal Cross Site Scripti				the first of the	ng/X546n7nummunt5	* \$ \$ \$	a a a a a a a a a a a a a a a a a a a
Create a new fiddle - /SFid ×   10 Create a new fiddle - /SFid ×   10 Create - 1 Cookies- > CSS- 2 First Create - 1 Cookies- > CSS- 2 First Cookies- > CSS- 2 Firs	5 Universal Cross Ste Scripti × Dapole edmon: 				the first of the	ng/klain/nummurf3	* \$ \$ \$	= = = * • • • • • • • • •
Create a new fiddle - //Fid × 4 Create a new fiddle - //Fid × 4 Control	5 Universal Cross Ste Scripti × Dapole edmon: 				the first of the	eg7k3ete/nummurt5	* \$ \$ \$	a a a a a a a a a a a a a a a a a a a
Create a new fiddle - /KFid * 12 Create a ne	S Universit Cross Site Scription (* ) Deptin annone (* ) Mageria controllogy (* ) (* ) Misse controllogy (* ) booard				A. Options-	eg7ไว้สอาวัฒนาการปร	* \$ \$ \$	a a a a a a a a a a a a a a a a a a a
Create a new Biddle - BFid × 2 Create a new Bid	S Universit Cross Site Souphi, S Objekti annur Site Souphing S States Schoology I I I I I I I I I I I I I I I I I I I			View Snurce- ) Quick Dra	A. Options-	ะรูวิจัรสิดวิณฑากอง75	* \$ \$ \$	a a a a a a a a a a a a a a a a a a a
Create a new fiddle - // Fid × 2 Constraint - // Constraint - // Constrain	S Universit Crocy Site Scrytt × Daptie amount			Wew Source-	A. Options-	ng7k5alan7kummauf5	* \$ \$ \$	a a a a a a a a a a a a a a a a a a a
Croste a new fidde - /SFid * 1 Conte a new fidde - /SFid * 1 Context unbase way Untarables Council for Bus Untarables Council for Bus Untarables Council for Bus Costboord Cos	S Universit Cross Site Souphi, S Objekti annur Site Souphing S States Schoology I I I I I I I I I I I I I I I I I I I			View Snurce-   Quick Dr. Title	A. Options-		* \$ \$ \$	a a a a a a a a a a a a a a a a a a a
Create a new fiddle - /SFid × 1 Constant of the Control of the	© Universal Crose Site Souptio, ≤ Oupdate ammun ser i for ages i for formation i for Mace echnology ♥ 0 ↓ New board ance Pages was 4.1.1 running evolve theme.			View Snurce-   Quick Dr. Title	<u>n</u> , Optices-		* \$ \$ \$	a a a a a a a a a a a a a a a a a a a
Create a new fiddle - /KFid × 2 Constraint - /KFid × 2 Constraint - /KFid × 2 Constraint - / Constraint - / Const	© Universal Crose Site Souptio, ≤ Oupdate ammun ser i for ages i for formation i for Mace echnology ♥ 0 ↓ New board ance Pages was 4.1.1 running evolve theme.			View Snurce-   Quick Dr. Title	<u>n</u> , Optices-		* \$ \$ \$	n 🗇 🖉 🚽 n 👘 🖓
Create a new fiddle - /SFid × 2 Constant of the catheod with a gas array with Constant of the catheod council for the catheod Constant Council for the catheod Constant Council for the catheod Constant of the cathe	S Universit Crock Stre Scripti	Hanesur 🥖 Duther 🧳		Quick Dra Title What's r	nj Options- aft		* \$ \$ \$	n 🗇 🖉 🚽 n 👘 🖓
Create a new fiddle - /KFid × 2 Constraint - /KFid × 2 Constraint - /KFid × 2 Constraint - / Constraint - / Const	© Universal Crose Site Souptio, Sr. Objektion animum ser Site Information- Site Macco echnology ♥ 0 ← News board annee Pages ways 4.1.1 running evolve themes.	Hanesur 🥖 Duther 🧳		View Snurce-   Quick Dr. Title	nj Options- aft		* \$ \$ \$	n 🗇 🖉 🚽 n 👘 🖓
Create a new fiddle - /SFid × 2 Constant of the catheod with a gas array with Constant of the catheod council for the catheod Constant Council for the catheod Constant Council for the catheod Constant of the cathe	S Universit Crock Stre Scripti	Hanesur 🥖 Duther 🧳		Quick Dr. Title What's c	n, Options- aft en yesur mir		* \$ \$ \$	a a a a a a a a a a a a a a a a a a a
Create a new fiddle - /SFid × 1 Context a new fiddle - /SFid × 1 Context /SFid × 1	S Universal Crock Site Scapelie, S Daptier amount in the second state of the second s	ikoronie 🥬 Dukor 🤌		Quick Dra Title What's r	n, Options- aft en yesur mir	nt?	+ 会 臣 * Berreen Opti	- CT
Create a new fiddle - /5Fid × ()	bill Universal Croses Site Scripti	ikoronie 🥬 Dukor 🤌		Quick Dr. Title What's c	n, Options- aft en yesur mir		+ 会 臣 * Berreen Opti	a da anti-
Create a new fiddle - SFid × 2 Control of the cathed of the as an array cather & Control of the cather Control of the cather Contr	S Universal Crock Site Scapelie, S Daptier Samon S Scape S Information S Marce School (2) S Scape S Scape S S Scape DOM New Cookies ( COS Script DOM New Cookies ( ( Cookies) -	ikonnie / Cuthor /		View Source -   Quick Dr. Title What's d What's d WordPre	aft aft sti yosur mir ss News	ndf? I Strench withou Counting p	+ ☆ 応 + Bereen Opt	
Create a new fiddle - /SFid × 2 Create a new fiddle - /SFid	bioiversal Crock Site Scapita, sr Dapties amount a	ikonnie / Cuthor /	Reise (C Tools III	Quick Dr. Title What's c	n, Options- aft en yesur mir	nt?	+ 会 臣 * Berreen Opti	
Constant a new fielde - SField  Constant a new fielde - SField  Constant - SField  Const	biological Crock Star Scapit v Destine amount in the scapit v Destine amount in the scapit v Destine amount in the scapit in the scape in the scale in the sca	Hannesser / Oudhor- /	Reise (C Tools III	View Source- ( Quick Dr. Tribe What's a WordPre	aft orr your mir or ss News News	167 P Search author Cantage	+ 会 的 ま former Option	
Create a new fiddle - SFid * * * * * * * * * * * * * * * * * *	bioliversal Crock Site Scripti		Raties (C Tooks )	View Source- ( Quick Dr. Tribe What's d What's d WordPree Bonson Bodiest	aft aft sh your min sh your min	P Steren with a Castary (	* \$ Borreen Option	
Create a new fiddle - /SFid * () Control in Control of Section 2015 Control of Control of Control Section 2015 Control of Control of Control Section 2015 Control of Control of Cont	biliversat Crock Site Scripti	Hennesse / Durline /	Raties (C Tooks )	View Source - ( Quick Dr. Tibe What's e What's e WordPre WordPre	aft options- off stryour mir ss News Ss News Ss News Ss News Ss Ss S	JD Search written Cauties J D Search written Cauties J Arthous approval Arthous approval	+ ☆ 応 * Ecreen Opt	
Create a new fiddle - SFid × 2 Control of the calibration of the sense servery alter - La Constance - Councel for Barry Constribution Councel for Barry Constribution Councel for Barry Constribution Councel for Barry Methods Posts Methods Pages Constribution Cons	biliversat Crock Site Scripti	Hanesus- / Outline- /	Raties (C Tooks )	View Source - ( Quick Dr. Title Webath o WordPre: Commen Societa Societa	aft orr your min ors News SS News News SS News	1077 P Sterreb wither Castras ( Path and gave a long adam, Act and gave and Act and gave and	・ ☆ 応 ・ Ecreen Opt	

Fig 7. Session fixation vulnerability

**4. File Upload Vulnerability:** It is observed that the application does not validate the file type being uploaded to the server. An attacker can upload malicious files which may lead to Remote Code Execution and the total defacement of the Web Application.

	Fire Applicate						-	
🛨 🥃 1 OCE Bahradan pre	unt in status	Contractions						
ingenitie - Mary Britter			an + 11	1 df (5) have	0.01	* 1	 1.00	- =
Trendra: Description Descript	An pringe An an	Figure constraints to one derive charac- ter and constraints and ter and constraints and ter and constraints ter and constraints ter and constraints ter and constraints ter and ter and ter and te	Figure Vice source and the source of the source of the source of the source with the source wi	 p files anywhere to upload				-
				maximum resident frames from the				

Fig 8. File upload vulnerability part 1



## ISSN: 2277-9655 Impact Factor: 4.116



Fig 9. File upload vulnerability part 2

**5. HTML Injection:** HTML Injection attack, closely relates to XSS, occurs due to inadequate validation of the input data into the web application and at the input fields where the input entered by the user is displayed back in user browser after the submitted data was processed at the server side. For example: 1. User submits a web page with field Full Name with the input text as John Smith. 2. Server receives the submitted data and responds to the user browser Welcome, John Smith. If the input field is not properly sanitized or validated, malicious user could insert a HTML Tags like which should execute on the browser to display an image. HTML Injection however, can exist due to input from GET, POST sometimes even HTTP headers when used in the server response by the application.[9][10][11]

Provident - procession		1 at 11 m August	0	m +		* *	
	benetiter @ Mandament / Deller / Second Streter # Test				20.000		-0
49 Million Street Converting Testar Streeting		and the second s		- Hunda	termine in		
	Pagement - Patterin - Manuel - Andrew Same	Street Street Street Stre					
					41	214	
	Second a linear a contract design and the line				-	100	
NORMA			Digni a				
and the second sec							
a second and	E State Stat						
a design of the second s	Testing Hacked						
- Andrewson							
- 94841							
Bir Viliage							
Barroh Fadi							
Campro Mag	No. Consequences						
- Caree		(2-30)					
- 79144			12.10.0012				
Camera Ha			Description Count	10 m			
True for Date of Determine			Revelating: Utauthant Coard	M			
- Magaza			And the second second second				
- Mere'rs Panis			ALC: NO WE WAS ADDRESSED		-		
19852							
					_	10000	
Recordings (19)							
Racotholys 1921	second in 200 h		Deseratorial Links			the second	

Fig 10. HTML injection vulnerability



## ISSN: 2277-9655 Impact Factor: 4.116

**6. Iframe Injection** : Tag stands for Inline Frame and is used to insert contents from another website or server. It is observed that application is vulnerable to Iframe injection. This injection is performed with html's Iframe tag which is inserted into the vulnerable area of the application. Vulnerability occurs due to inadequate data validation controls within the application.[12][13]

Statistics and the second second		- # 1 = 1 = 1	· · · · · · · · · · · · · · · · · · ·
	tenter 🔤 bespter 🔕 Mitanistico 🙀 Mitalteneous 🥒 Statue 🖉 Rester 🗶 Tenter 🗰 7	new paracter (A) Dataset	
The Arthread Concerning Star	technicka 🐨 1 - 🖶 tere		Thready, Second Second
A date			Stream Chattan +
Pibli	New Post		
Tes	ang for itrame injection ">		

Fig 11. Iframe injection vulnerability

**7. Insufficient Transport Layer Protection(SSL/TLS):** Insufficient Transport Layer Protection is a security weakness caused by applications not taking any measures to protect network traffic. During the authentication, applications may use SSL/TLS, but they often fail to make use of it elsewhere in the application, thereby leaving data and session ID's exposed. Not using SSL/TLS at all throughout the application, leaves the application open to sniffing of usernames and passwords by an attacker. Sometimes applications are deployed using weak certificate algorithms, expired or invalid certificates, or do not use them correctly. [14][15][16]

On 1991 (Des. 1999) (Descent) (Delt. 1991		
	/ O-torracting	*(+)
+ P It hidest with produce security		
	tanahar 📷 Maraharanan 🥖 Salar 🥒 Baran 🖉 Yana 🗰 Yan Jar	auto state tropped at 11 au
		Annual States Concernence (Second States)     Annual States (Second States)     Annual States (Second States)     Annual States (Second States)
	0	Compared to the product of (100.00.0)
	No.	Total frame frames frame
	Charline Test	Oreno Astrono - Brazilari A.H. (Bilandryn MT. 4, 21) (MURCH, 2010 M. 2010 M
	testin	(Werkenstein Steiner / / Loss Charter (aufe, aufe, auto,
	Partmented	Concerner Types, applicant control and form on intermediate
	******	Ligences impairment impairment to a similar to get interestations, to sho pet laster.
	13 American Ale	- \
	a state part of the second secon	Louis a sumbound and and he plants must
	<ul> <li>A set of the intervention of the set of th</li></ul>	
and the local division of the local division of the		The second se

Fig 12. Insufficient Transport Layer Protection vulnerability

**8. Improper Cache Control:** Improper cache control vulnerability occurs due to improper implementation of cache control directives. It happens when sensitive data get stored in browser cache and it is possible to access authenticated pages of the application after logout, specifically from the history of the browser in offline mode. For example: 1. A user visits to his profile after authentication and views some internal pages that have some sensitive information like credit card number or social security number and then logs out of the application. 2. Later, an



[Kumar\*et al., 5(8): August, 2016]

#### IC<sup>TM</sup> Value: 3.00

## **ISSN: 2277-9655**

**Impact Factor: 4.116** 

attacker with access to victim's computer can view restricted pages previously accessed by the victim from history or the cache of the system.[17][18]

E B Model and an arrest element	tota point 1990 her men stilling weren fit	n (e)		+ 白 府 弗 甫	# 1 m 3
Comments of the state of the st		flather A fame of fame in the lands. A fighter	#11	and the second se	10
	🕈 Internet Constitute Designation 🐨	1 -+ WW VierPert			and ing bender 🔒
Pacadout (printing) to a trans	Edit Post Anno	-		teriet teter. *	Colora To
Stouthanijertegihilijet.	Plat IT IT Low Sector Plat	e-me parts			
in ann graph to to a fist-					
Dises googk is to offer a		w.post*>~syg/onload=alerti/X5S/)		Publish	
D weet-people of the first -	the second s	to of a lot testilation of the set of the sub-side to be balance of			
US united - taines, set all.	Permately fattering to	which are related to the		Same Dirate	Course -
Character Assessment Character	All Antonia All In	menter 🗮 ment succession . And has made in the	· Of Address	* Transit Grant Lass	
Alread as (10%-indexed Co	Tall standards		- In success		
Add Sam Roll - Officialia.	g11		TOTAL TANK	op. monolity Padde 1200	
	Tell - Cash Country	the set og is to be set toes	there is a local sector	The Public Interestivity [10]	
Constant Interactions	A CATALON CONTRACTOR OF CALL			PEASELING	-
Contraction of participation of the second s		**alignment***align************************************		takive to main	Patricip
	weite Gallery Schapting	structs, addances, to adventual must an			
Light Page 1 Milerahrsend Co.	and the second second			Permat	
Lat Post - Management Con-	generative digit.			A COMPANY AND A	
Balt Mary - MaryMand Co.	49115			· P Handard	
Rote Line - Litracultured Co.	and the second se			C1 ()] 4444	
er nodens	and the second se	secondly without		CI 13 hote	
d Postage Address for Fost.				CI The Oral	
Changes III-S	terms.			Cl III Index	
Trate of General				(1) [1] here	

Fig 12. Improper Cache Control vulnerability

**9. Login Brute Force:** It is observed that login page does not restrict multiple failed login attempts. A brute force attack is a method to determine an unknown value by using an automated process to try a large number of possible values. For example: While an 8 character alphanumeric password can have 2.8 trillion possible values, many people will select their passwords from a much smaller subset consisting of common words and terms.[20]

P 12 headwall in the annual sector wanted		1.61			+ 4	2 41 4 W.	
halder & Contrast of 120 12 Name in Surgary () Information () 10	estemar / Caller / tes				PERSONAL AND A		
		Area have determ					
		Details. To at feature. As	and from 1				
and the second second		The investigation					
Login respect with invalid parament. Status		Interest in Payment	Summer (		The later		
	1	1 BANK OF	300		199	÷	
		A passon of the	200	i i i		÷	
Large response with radial permanel. Sparse and a large		Citerina Social		0	- T	1.1	
1012 Frank, which is an investigation	STREET, The party of the second secon			-	1111220		
	administration of the second s	Ram Handbill Bar					
		Trans. Mile, 17 Add. Trans.	TINE LA LOUT				
	Children and Child	Direct space/2.2.1.14 /8 and space/ Directorial's.7. A-Finders-Fr. FET.5.7.1	a short gray sol . D.	L tors	S. St. Openiti	LIG. S. SI motor	a
		Repaires. Red. 15 Jan 1909 Tanto Construct Strengton,	a statisticate core		1000		
	warlock	Prochast don-parks				Tanks of Lands and	
	(Palataint)	And the last has for-					
		Traini I					
	•••••	CAMPE.					
		WARES.					
	•••••	CAMPE.					
	•••••	CAMPE.					

Fig 13. Login Brute Force vulnerability

#### 3.3 Removal of Vulnerabilities:

**1. Improper Session Termination, Improper Cache Control & Session Fixation:** Vulnerability due to improper cache management solved. File location \wp-include.php Line no 1003-1040. The code below represent the affected area.

\$headers = array( 'Expires' => 'Wed, 11 Jan 1984 05:00:00 GMT', 'Cache-Control' => 'no-cache,no-store,private,precheck=0,post-check=0, mustrevalidate, max-age=0', 'Pragma' => 'no-cache', );



**2. Stored Cross-Site Scripting, HTML Injection & Iframe Injection:** Removal of HTML, XSS and iframe injection in post –title field in admin dashboard using input sanitization on title field. File location \wp-includes\post-templates.php. (line no 78-162). The code below represent the affected area.

\$title = \$r['before'] . \$title . \$r['after']; \$title = esc\_attr( strip\_tags( \$title ) ); \$title = sanitize\_text\_field( \$title );

**3. File Upload Vulnerability:** Removal of FILE upload vulnerability by removing HTML & .exe files from allowed file types. Location of file /wp-include/functions.php and the code can be found b/w line no's 2164-2277. //'htmlhtml' => 'text/html',

//'exe' => 'application/x-msdownload',

**4. Insufficient Transport Layer Protection(SSL/TLS), Login Brute Force and Weak Password Policy:** These issues were removed using all in one wordpress security plugin.

**5.** Cookie Secure and HTTPOnly Attributes Not Present: The cookie secure and Http functions were enabled. File location \WP-confg.php.

@ini\_set('session.cookie\_httponly','On'); @ini\_set('session.cookie\_secure','On'); @ini\_set('session.use\_only\_cookies','On');

**6.** Auto-Complete Feature Enabled: To disable auto-complete feature we implement two changes: a) First change in functions.php:

function kill\_autocomplete() {
 wp\_register\_script('kill-ac',
 get\_template\_directory\_uri() . '/js/autocompleteoff.js',
 array('jquery'),
 '1.0');
 wp\_enqueue\_script('kill-ac');

}

add\_action('wp\_enqueue\_scripts', 'kill\_autocomplete');

b) Second change is in /js/autocompleteoff.js: jQuery('#user\_pass').attr('autocomplete','off');

7. Http Method Enabled: The http method is disabled from .htaccess file as follows:

# Rules to block unneeded HTTP methods

RewriteCond %{REQUEST\_METHOD} ^(TRACE|DELETE|TRACK) [NC] RewriteRule ^(.\*)\$ - [F]

#### 3.4. Scanning <u>http://www.ucb.uk.gov.in</u> using online vulnerability scanning tools:

**1.** Google safety diagnostics tool: The scan results shows that the website is safe and not dangerous.

	Google Tr	anaparency	Report		the state of the s
			Assessing and private		
	Physical Division Street	Sale Honory of	and attack		
	Transie Wennen der Heuten With Heller Hann Pag	and distantly biogeneously a	teriendagi asarahan alkera at 1994 an fanan mang yang, wan ya salah at 1 mang yang yang yang yang yang yang yang i tahukung tahun ya tahun ya tahun yang yang yang yang yang yang yang yan	n may Bastraph For screptio antibules. Form - Ha- generative vanishish, Bart Name Neer In Mangar Samah, and in and Hammann, Nam International Samah Samah Samah Samah Samah Samah International Samah Sama Samah Samah Sam	
		Bits beforg breats Date page of the Magnine establish	marke over the set of the lateration	Functing designs the set operand are information about article groups in August prior. This instantion to function of Elbert energy	-
1	-				4.0 米 ¥ m

2. Norton safe web vulnerability scanner tool: The scan results shows that the website is safe.

**3. Beyond security online vulnerability scanner tool:** The scan results shows that the website is safe with vulnerability score 81.

#### ISSN: 2277-9655 Impact Factor: 4.116



# [Kumar\*et al., 5(8): August, 2016] **ICTM Value: 3.00**

## **ISSN: 2277-9655 Impact Factor: 4.116**

## **RESULTS AND DISCUSSION**

This work is an attempt to develop a secured wordpress website in which after the basic installation the it was tested according to OWASP, SANS, WASC standards[4]. The flaws in the security were cleared to maintain the website security. The corrected code were applied to the related wordpress file and the updated wordpress was then reaudited to check the vulnerability status. The results of level 2/final website security audit report is as follows:

Vulnerability Name	Severity	Status
Improper Session Termination	Flah	
Stored Cross-Site Scripting	High	23
Session Fixation	High	23
File Upload Vulnerability	High	63
HTML Injection	High	2
Iframe Injection	High	23
Insufficient Transport Layer Protection(SSL/TLS)	Medium	
Improper Cache Control	Medium	
Login Brute Force	Medium	
Cookie Secure Attribute Not Present	Law	A
Auto-Complete Feature Enabled		<b>A</b>
HTTPOnly Attribute Not Present	Low	-
Weak Password Policy		2
Http Method Enabled	LOW	A

#### Table 2: Details of final security audit report

💟 = Fixed

Business Exception

The website www.ucb.uk.gov.in is safe and secure according to National Informatics Centre security audit vendor report and is safe for hosting at NIC platform. For the sake of counter verification the website was also audited from online vulnerability diagnostic tools and some of the reports also confirm the safety of the website. After this work the wordpress recently had been updated to the wordpress version 4.5.2 along with hardened .htaccess, php.ini and other security measures to compete with the latest vulnerability issues. And the current status is also safe and secure.

#### REFERENCES

- 1. Rushabhkumar H. Baldaniya and Prof. H.J.Baldaniya, 2014 "Web Development Using Content Management System", International Journal of Emerging Research in Management & Technology, April 2014, ISSN: 2278-9359, Volume-3, Issue-4.
- 2. Vimal Ghorecha and Chirag Bhatt, 2013 "A guide for Selecting Content Management System for Web Application Development", International Journal of Advance Research in Computer Science and Management Studies Research Paper, August 2013, ISSN: 2321-7782, Vol. 1, Issue 3.
- 3. https://en.wikipedia.org/wiki/Wordpress, 20 August 2016.
- 4. https://en.wikipedia.org/wiki/Web application security, 20 August 2016.
- 5. https://www.owasp.org/index.php/Testing\_for\_Logout\_and\_Browser\_Cache\_Management\_(OWASP-AT-007), 01 may 2015.
- 6. https://www.owasp.org/index.php/Testing for Stored Cross site scripting (OTGINPVAL-002), 01 may 2015.
- 7. https://www.owasp.org/index.php/Session\_fixation, 01 may 2015.
- 8. http://cwe.mitre.org/data/definitions/384.html, 01 may 2015.
- 9. https://www.owasp.org/index.php/HTML Injection, 01 may 2015.
- 10. https://www.owasp.org/index.php/HTML\_Entity\_Encoding, 01 may 2015.
- 11. http://php.net/manual/en/function.html-entity-decode.php, 01 may 2015.
- 12. https://www.owasp.org/index.php/Cross Frame Scripting, 01 may 2015.
- 13. http://resources.infosecinstitute.com/iframe-security-risk/, 01 may 2015.



## [Kumar\*et al., 5(8): August, 2016]

## ICTM Value: 3.00

## ISSN: 2277-9655

**Impact Factor: 4.116** 

- 14. https://www.owasp.org/index.php/Top\_10\_2010-A9-Insufficient\_Transport\_Layer\_Protection, 01 may 2015.
- 15. <u>http://projects.webappsec.org/w/page/13246945/Insufficient%20Transport%20Layer%20Protection</u>, 01 may 2015.
- 16. <u>http://www.troyhunt.com/2011/11/owasp-top-10-for-net-developers-part-9.html</u>, 01 may 2015.
- 17. https://www.owasp.org/index.php/Testing\_for\_Browser\_cache\_weakness\_%28OTGAUTHN-006%29, 01 may 2015.
- 18. <u>http://condor.depaul.edu/dmumaugh/readings/handouts/SE435/HTTP/node24.html</u>, 01 may 2015. <u>https://www.owasp.org/index.php/Blocking\_Brute\_Force\_Attacks</u>