



## International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018

# Advanced Web Penetration Testing Using Kali Linux

Subarna Panda, Bokobri Lekpeli Koissy Franck Olivier

M.Tech, Assistant Professor, Department of Computer Science and Information Technology, Jain University,  
Bangalore, India

MCA Student, Department of Computer Science and Information Technology, Jain University, Bangalore, India

**ABSTRACT:** Security of web application has become more gradually important in our digital world. Many and dangerous attacks are deployed against web application among those attack as per report of web application SQL injection is the most executed attack against web application. As the usage of web application increase the web application gets vulnerable to many threat which is a serious issue which need to be address to enhance the security of web application. One of the major threat of web application is the poor coding during the development. Many security solution exist for securing a web application such as WAF (Web Application Firewall) but which remain inefficient as the weakness exist in the web application coding. Finding the suitable security means to protect the web applications as well as the company asset remains performing and excellent and advanced penetration testing on the web application to find the flaws which susceptible to cause enormous damage to the web application and fix it at the development phase of the web application. Our task will be to perform an advanced penetration testing for the web application to enhance drastically his security features.

**KEYWORDS:** Server-side Request Forgery, Common Weakness Enumeration, Cross-Site Scripting

### I. INTRODUCTION

Web application is client-server program or software which run on a web server to provide different services and is accessible by using a web browser. A security assessment conduct by Q1 showed that 19,889 maximum number of attack in a day occurs against single company and the top of those attack is SQL injection. Another security assessment conduct by IMPERVA shows that the number of vulnerabilities on a monthly basis over the last two years has increase significantly from 6,615 in 2016 to 14,082 which is around 212% and cross-site scripting are the majority in 2017 web application vulnerability. A web application remains the top prime vectors for criminals because of sensitive data. Various security means has been deployed by organization to secure their web application among them web application firewall which is deploy as traditional firewall into the network. The issue with those technologies is they can't secure the web application when the attack is sophisticated. Another issue face by web application is the third party application which is connected to them, even if the main web application is correctly secure the third party application can become easily a threat for the web application and however need to be address.

### II. RELATED WORK

[5] VAPT (Vulnerability Assessment and Penetration Testing) is a comprehensible service for auditing, penetration testing, reporting and patching company web applications. As many company run their business online and which is involve web application the port 80 which remain open is a door open for attacker. As the 80 port is open there is a chance that attacker find a use a flaw in the system to hack the company's web application and network. A small precision but necessary one is vulnerability assessment and penetration testing are two different approach. The vulnerability assessment the security posture of the information system both internally and externally on the other penetration testing provide evidence that vulnerabilities do exist as a result network and web penetrations are possible. VAPT can be defines a systematic analysis of security status of information system. From that definition vulnerability



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018

assessment offers partial evaluation of vulnerabilities and penetration testing is the practice of testing a computer system network or web application to find vulnerabilities that an attacker could exploit.

Penetration testing can be automated (software Application) or manually done by penetration tester. Gathering information about the target and identifying potential entry are some task which is perform by penetration tester. The goal of penetration testing is to determine security weakness and can be used to test organization's security policy compliance, employee's awareness and organizations to identify and respond to security incidents. The methodology is divided into various section as follow: Discovery, Enumeration, vulnerability identification, exploitation and launching of attacks. Vulnerability analysis consist of following steps: Defining and classifying network or system resources. Assigning relative levels of importance to their sources. Identifying potential threats to each resource. Developing a strategy to deal with the most serious potential problems first.

Information security can't be neglected in any area particularly important in the finance sector not only because of financial sector but client and organization process sensitive information. As a way the organizations need to test their security in infrastructure, networks, web applications and many others , the company need penetration testing to evaluate the security which is currently implemented. Penetration testing is implemented because simulates an attacker's behavior in a controlled environment in order to identify its vulnerabilities.. The penetration testing methodology for this case is as follow: Setting up web scanner configuration, Navigate through the web application, Perform the crawling, Explore the web application crawled pages, Perform fuzzing on the web application pages, explore the application logic parameters, Exploitation, Mitigations and Reporting. The penetration testing for the financial application found broken authentication, Cross-site scripting, Insecure Direct Object Reference, Sensitive Data Exposure, and Invalidated Redirects and Forwards. The adoption of a methodology and security controls in all SDLC and organization processes is recommended such as Building Security in Maturity Model (BSIMM), OWASP Application Security Verification Standard (ASVS), OWASP Software Assurance Maturity Model (SAMM).to reinforce the security of any software some security controls should be implemented such OWASP proactive controls such as Verify for Security Early and Often, Parameterize Queries, Encode Data, Validate All Inputs, Implement Logging and Intrusion Detection, Leverage Security Frameworks and Libraries, Protect Data, Implement Identity and Authentication Controls, Leverage Security Frameworks and Libraries, Error and Exception Handling.

### III. SYSTEM ARCHITECTURE

The system architecture is a central part of our work which is to find some vulnerabilities in the web application system. In fact the system architecture use for the advanced penetration testing is a 64 bit architecture which means more fast for executing task and many others advantages which is essential for our work. The system architecture is divided into different modules such as the applications. The applications gather many applications which will be used for penetrate and exploit some vulnerability found in web application. The system architecture include the libraries which are resources used by computer programs to I order to add more functionality to an existing software or can be used to develop software itself. The libraries are non-volatiles resources. The IPC (Inter Process Communication) allow different programs to interact which each by exchanging information and share memory. The network module is responsible for all task related to network such as sending and receiving message from host, coding and decoding bit, framing bit and many other functionality related to network. Other modules such as process management responsible of allocating process, sequencing process, initialize process and even destroy a process is useful in the system architecture similar to memory management which allocate memory to process, delete unused memory. SELinux is a modules responsible for providing access control security policies. SELinux is the implementation of Mandatory Access Control, SELinux verify allowed operation after a discretionary access controls. It includes many features such as policy interfaces, security for socket, messages and network interfaces and finally security for process initialization and inheritance and program execution. The other modules are very helpful for the system architecture. Kali Linux is a debian distribution and so kali Linux have the same features with debian and apart from the debian features kali linux have its own feature which are ARMEL and ARMHF support it mean that kali can run on devices such as raspberry pi, beaglebone and others ARMEL and ARMHF devices which are inexpensive. Before kali Linux backtrack 5 was available to do penetration testing which was not well integrated with the hardware and some issue was found when running some applications but now with kali Linux there is a full integration hardware which make kali Linux great and good features such as complete customizable, custom kernel, and great enhancement kali Linux support wide ranging

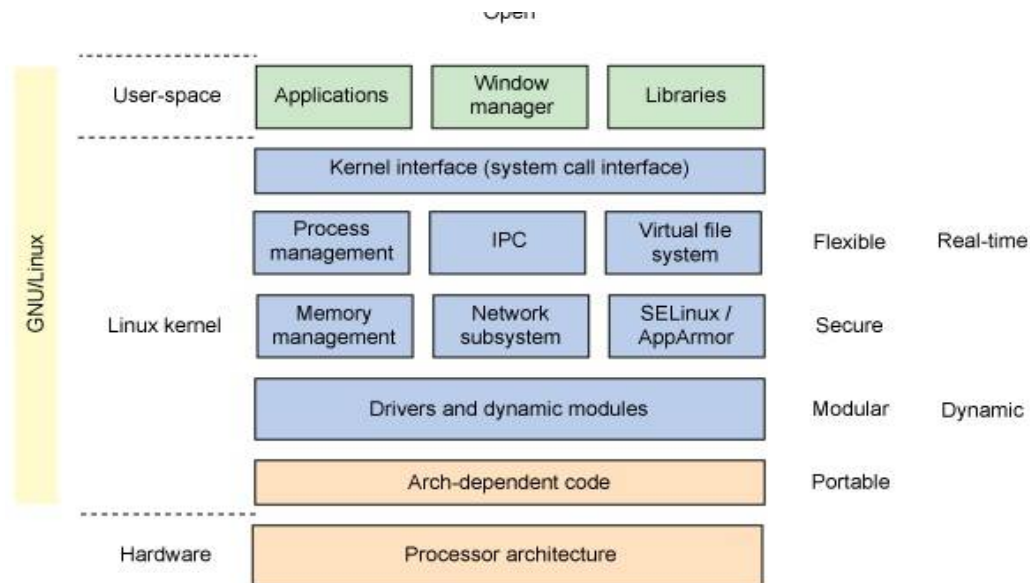
# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijirccce.com](http://www.ijirccce.com)

Vol. 6, Issue 4, April 2018

wireless device, and the most important update is more than six hundreds testing tools which is very impressive. Some others feature such as open source Git tree and file system Hierarchy standard



## IV. APPROACH OVERVIEW

The approach follow for the advanced penetration testing is defined as following:

### IV.1 Gather Information

Gather information is a process which consist to collect information on a specific target. The information gather in this phase should be helpful for the upcoming phase. Examples of information which need to be gather is the technology used by the web application such as technology implemented at client side and server side which can be JavaScript, CSS (Cascading Style Sheets), React, Angular or any technology at client side. The information which can be collected for the server side might be the operating system user for the web server, DNS information, programming language, IP range and many other information which can be useful for further penetration testing. Gathering information which help to further find specific vulnerabilities to the web application. Information gathering can be passive in the sense where there is no contact with web application or the company, those information can be find in public information such as news, recent technology upgrade and public report provided by company having the web application.

### IV.2 Vulnerability Gathering

Vulnerability gathering is the second process of the advanced penetration testing which consist to collect the vulnerability of the technology used by the web application. Enumerate the vulnerability from client side to server side. The vulnerability also is done purely manually by using some international common database for vulnerability such as CVE database, CWE database, and NIST database. This vulnerability will show to the penetration tester what the latest vulnerability of the technology are and will be able to locate and exploit them if some exploit framework is available or exploit them manually. Vulnerability gathering is crucial process for the advanced penetration testing because, the vulnerabilities collected in this phase have to be specific to the technology that the web application is using. As the database for vulnerability is huge a considerable time have to be consume on each and every vulnerabilities databases. As in the gathering information we get to know the technology used in the web application as an example JavaScript. The advanced penetration establish some gap analysis between the current version used and the latest version. The advanced penetration testing then identify the vulnerability for the current version either cross-site scripting, security misconfiguration, some flaws in the technology used, ddos attack possible because of certain aspect of the web



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018

application and many others vulnerabilities. This work should be done for every international databases vulnerabilities as the databases are different and the advanced penetration testing should identified all possible vulnerabilities which can cause damage to the web application. The vulnerabilities found in this process which has not get approval from the senior management should not be exploit but mention in the final report.

## IV.3 Gaining and Penetration

Gaining and penetration process will consist to exactly exploit the vulnerability found in the previous stage. This process will begin by get some more vulnerability using tools such as web vulnerability scanner. It will help to find other vulnerability which are not find manually during previous stage. All the vulnerabilities is use for addressing in first place the top ten threat define by OWASP which a nonprofit organization other vulnerability will be address even not include in OWASP top then threats. Penetration consist of exploiting the vulnerability found early. Gaining and penetration testing is a crucial process where the asset the web application is tested. The advanced penetration testing should stay in the border defined during the agreement of the penetration testing because some attack against the web application could shut down the web application before those attack is lunch, the attack must have permission from the senior management. As an example of gaining and penetration testing sql injection which is a major vulnerabilities for web application exploit some vulnerabilities and allow the penetration tester to access to the database once the database is accessed then many attack is possible like bypassing authentication mechanism and sensitive data exposure. For each vulnerability identified in previous process it should be exploited according to the limit and using a framework called metasploit It is a good practice to have metasploit framework update because it help to address those vulnerability. Once gained access to web application method of accessing should be correctly document in the final report.

## V. REPORTING

Reporting is the last process for the advanced penetration testing. It allow to make a details report about the vulnerability found in the web application. The report should address the OWASP top ten, it should mention if the threat has been identified in the web application or not and follow by the POC (Proof Of concept), the affected URL and the severity. The reporting is traditional process after the penetration is exactly done. The report should be well made and more understandable by the senior management but also by the developer because after so many findings which could cause damage to the web application so adding more secure programming to the web application is necessary depend on the severity of each vulnerabilities. The final report should have color based of the severity of each vulnerabilities on a scale of ten. The severity of each vulnerability should be categorize between low, medium and high to better understand his impact. The report should be deliver to the concern authority.

## VI. IMPLEMENTATION OF ADVANCED PENTERATION ON TARGET (OWASP TOP TEN THREAT)

The OWASP top threat for web application define the major threat that web application can face and those threat can cause damage to the web application if not proper develop. The top then address in our work is OWASP 2017.

### VI.1 SQL INJECTION

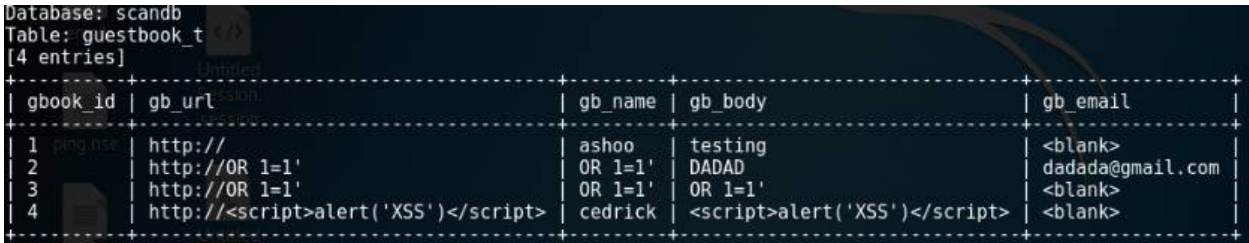
Sql injection is an attack which consist to inject some malicious sql queries to the web application. The sql injection is implemented by inserting the malicious sql query into an input field of the web application or by using an automated tools. SQL injection exploit some vulnerability in the web application and have for specific target the database used by the web application. SQL injection is considered as by OWASP as number one dangerous attack against web application. Performing an sql injection require to test if the web application is vulnerable or not to sql injection by adding “ ‘ “ or leveraging the URL parameter of the web application. The quote given to the web application URL will confuse the database and the web application will throw an error because the database doesn't how to handle the query. The result of a sql injection against a web application is as the following:

# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018



```
Database: scandb
Table: guestbook_t
[4 entries]
+-----+-----+-----+-----+-----+
| gbook_id | gb_url | gb_name | gb_body | gb_email |
+-----+-----+-----+-----+-----+
| 1 | http:// | ashoo | testing | <blank> |
| 2 | http://OR 1=1' | OR 1=1' | DADAD | dadada@gmail.com |
| 3 | http://OR 1=1' | OR 1=1' | OR 1=1' | <blank> |
| 4 | http://<script>alert('XSS')</script> | cedrick | <script>alert('XSS')</script> | <blank> |
+-----+-----+-----+-----+-----+
```

Fig.1 SQL INJECTION

Here the web application was vulnerable to sql injection and some malicious sql query perform against the web application and we got the above result.

## VI.2 BROKEN AUTHENTICATION

Broken authentication is another threat and technique which is use to bypass the web application authentication mechanism. As the now attacker have access to many username and password breaking the authentication mechanism become more easy for attacker. The attacker can use a brute force attack to bypass the authentication or dictionary attack. Both technique is the way that dictionary attack use a predefined list of username and password while brute force use all the possible combination to find the correct username and password which is an heavy process. A broken authentication has been performed on web application and the result is shown below:

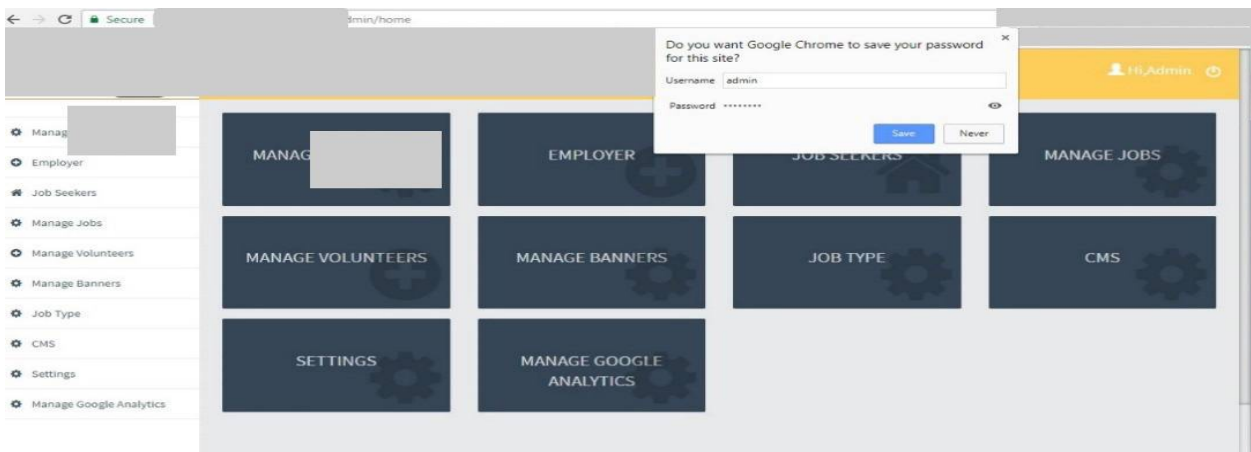


Fig.2 BROKEN AUTHENTICATION

## VI.3 SENSITIVE DATA EXPOSURE

Sensitive data exposure occupy the third rank for top ten threat of OWASP 2017 because sensitive data can be credit card, social security number, healthcare information username and password. For the web application sniffing tools can be used to retrieve data from the network if the web application doesn't use secure protocol such as HTTPS, SSL or TLS. To expose the sensitive data of a web application a sniffing communication has been set up using wireshark and tcpdump and we got the username , password and confidential data of the company for which the test has been performed, the result for the advanced penetration testing for sensitive data exposure is below :



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018

```

> Transmission Control Protocol, Src Port: 51960, Dst Port: 80, Seq: 1277, Ack:
> Hypertext Transfer Protocol
  HTML Form URL Encoded: application/x-www-form-urlencoded
    Form item: "__CSRFToken__" = "68f344e44e449be1447347a555fc45c939f6f998"
      Key: __CSRFToken__
      Value: 68f344e44e449be1447347a555fc45c939f6f998
    Form item: "luser" = "u357391: .net"
    Form item: "lpasswd" = "123456"

```

---

```

02d0 38 33 33 30 32 39 39 2e 31 35 31 36 36 30 38 39 8330299. 15166089
02e0 33 37 3b 20 70 6f 73 74 5f 69 64 3d 5b 31 31 31 37; post _id=[111
02f0 5d 2c 5b 31 31 31 5d 2c 5b 31 31 31 5d 2c 5b 31 ],[111], [111],[1
0300 31 31 5d 2c 5b 31 31 31 5d 2c 5b 31 31 31 5d 2c 11],[111 ],[111],
0310 5b 33 35 30 34 5d 2c 5b 33 35 30 34 5d 2c 5b 33 [3504],[ 3504],[3
0320 35 30 34 5d 2c 5b 33 35 30 34 5d 2c 5b 33 35 30 504],[35 04],[350
0330 34 5d 2c 0d 0a 0d 0a 5f 5f 43 53 52 46 54 6f 6b 4],... __CSRFToK
0340 65 6e 5f 5f 3d 36 38 66 33 34 34 65 34 34 65 34 en_=68f 344e44e4
0350 34 39 62 65 31 34 34 37 33 34 37 61 35 35 35 66 49be1447 347a555f
0360 63 34 35 63 39 33 39 66 36 66 39 39 38 26 6c 75 c45c939f 6f998&l
0370 73 65 72 3d 75 33 35 37 33 39 31 38 25 34 30 6d ser=u357 3918%40
0380 76 72 68 74 2e 6e 65 74 26 6c 70 61 73 73 77 64 'et &lpasswd
0390 3d 31 32 33 34 35 36 =123456

```

Fig.3 SENSITIVE DATA EXPOSURE

CONFIDENTIAL PRICE LISTING				
EFFECTIVE DATE: May 1, 2014				
Part Number	List Price	Weight (pounds)	Volume (cubic ft)	Description
F-1800	649.00	2	0.5	1800 CABINET
37-0	144.00	2	0.25	CURB/PANEL MOUNTED SINGLE GAV
37-0A	144.00	2	0.25	CURB/PANEL MOUNTED SINGLE AIR
37-0G	144.00	2	0.25	CURB/PANEL MOUNTED SINGLE GAS
37-0N	144.00	2	0.25	CURB/PANEL MOUNTED SINGLE NIT
37-0V	144.00	2	0.25	CURB/PANEL MOUNTED SINGLE VAC

Fig.4 Confidential information Disclosure

## VI.5 XML EXTERNAL ENTITIES

XML external entities is a threat for web application in the sense that the attack exploit a vulnerability in the XML processor. The exploitation of the xml processor can cause damage to the web application because xml file can malicious code and once the file uploaded the attacker can exploit the code in the xml file or exploit some dependency. XML external entities is a new major threat for web application defined in OWASP 2017 to ten threat. Modifying the URL from the browser directly allow the attacker to edit any content on the website. To demonstrate this attack we chose a vulnerable web application to show how the xml external entities can be exploit

## International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018



Fig.5 XML PROCESSOR VULNERABILITY EXPLOITED

### VI.6 BROKEN ACCESS CONTROL

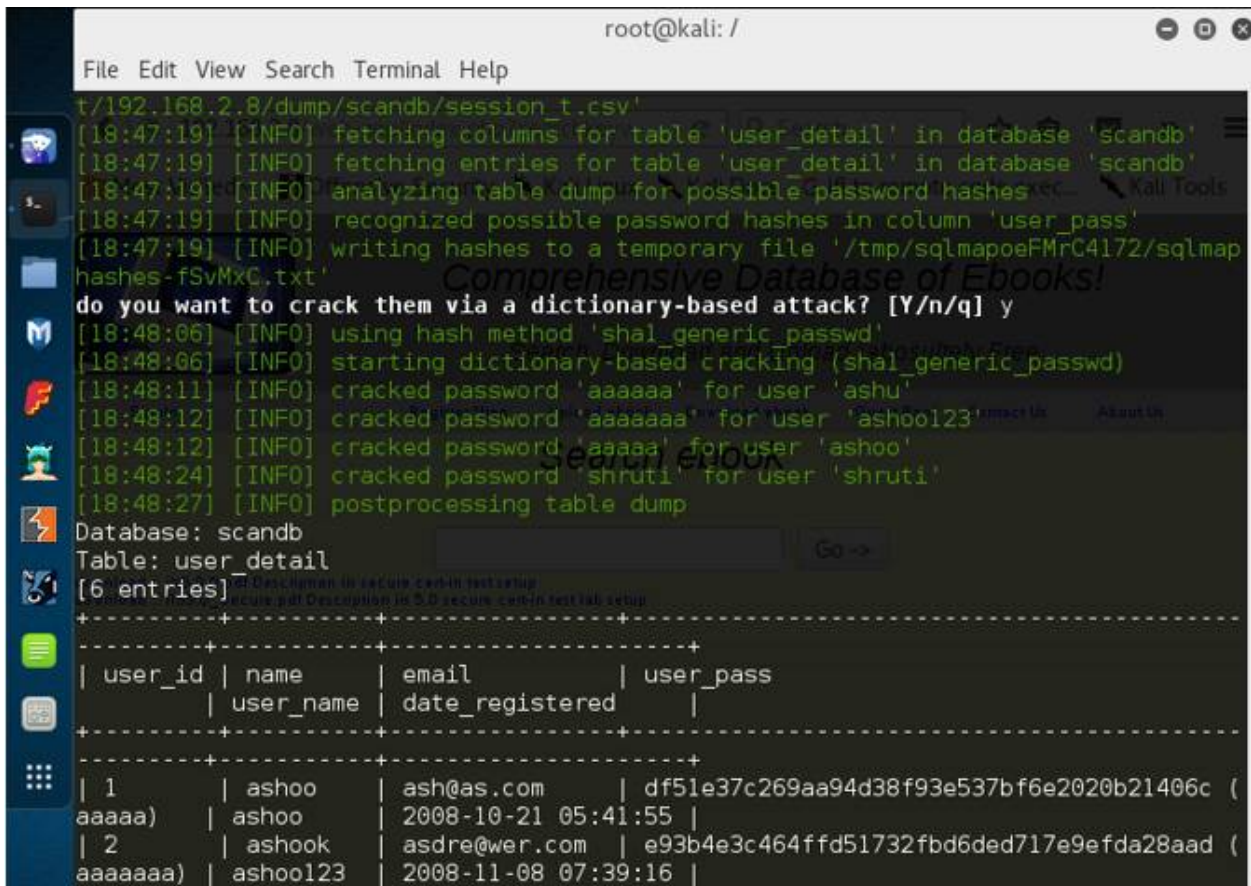
Access control is security mechanism implemented either physically or logically to prevent unauthorized access to object such as network, services, communications link, databases. Access control allow and use to prevent disclosure of information, alteration of information and maybe unavailability of resources from unauthorized user. An example of access control mechanism login system so broken access control remain a major negative impact for the web application. Advanced penetration testing used sqlmap to bypass the login page of a web application as following:

# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018



```
root@kali: /
File Edit View Search Terminal Help
t/192.168.2.8/dump/scandb/session_t.csv'
[18:47:19] [INFO] fetching columns for table 'user_detail' in database 'scandb'
[18:47:19] [INFO] fetching entries for table 'user_detail' in database 'scandb'
[18:47:19] [INFO] analyzing table dump for possible password hashes
[18:47:19] [INFO] recognized possible password hashes in column 'user_pass'
[18:47:19] [INFO] writing hashes to a temporary file '/tmp/sqlmapoeFMrC4172/sqlmap
hashes-fSvMxC.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[18:48:06] [INFO] using hash method 'shal_generic_passwd'
[18:48:06] [INFO] starting dictionary-based cracking (shal_generic_passwd)
[18:48:11] [INFO] cracked password 'aaaaaa' for user 'ashu'
[18:48:12] [INFO] cracked password 'aaaaaaa' for user 'ashool123'
[18:48:12] [INFO] cracked password 'aaaaa' for user 'ashoo'
[18:48:24] [INFO] cracked password 'shruti' for user 'shruti'
[18:48:27] [INFO] postprocessing table dump
Database: scandb
Table: user_detail
[6 entries]
+-----+-----+-----+-----+
| user_id | name | email | user_pass |
| user_name | date_registered | |
+-----+-----+-----+-----+
| 1 | ashoo | ash@as.com | df51e37c269aa94d38f93e537bf6e2020b21406c (
aaaaa) | ashoo | 2008-10-21 05:41:55 |
| 2 | ashook | asdre@wer.com | e93b4e3c464ffd51732fbd6ded717e9efda28aad (
aaaaaaa) | ashool123 | 2008-11-08 07:39:16 |
```

Fig.6 BROKEN ACCESS CONTROL USERNAME AND PASSWORD OBTAINED

The username and password can be easily seen on the capture screen so the credentials to login as admin and play the role of admin in the web application.

## VI.7 SECURITY MISCONFIGURATION

Security misconfiguration is another challenge and threat for web application. Security misconfiguration is listed top six for OWASP top ten. Security misconfiguration means some component of the web application has not properly set and which create some flaws in the web application. Unpatched component, non-used page, default configuration, default location and many more form security misconfiguration. Security misconfiguration may reside at the client side of the web application as well as server side some example of security misconfiguration at client can be improper input sanitization, X-frame options not enable, security protocol not implemented such as HTTPS, SSL or TLS or weak https which have a vulnerability in key exchange(DHE). Found vulnerability in a web application which is a security misconfiguration:



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijirce.com](http://www.ijirce.com)

Vol. 6, Issue 4, April 2018

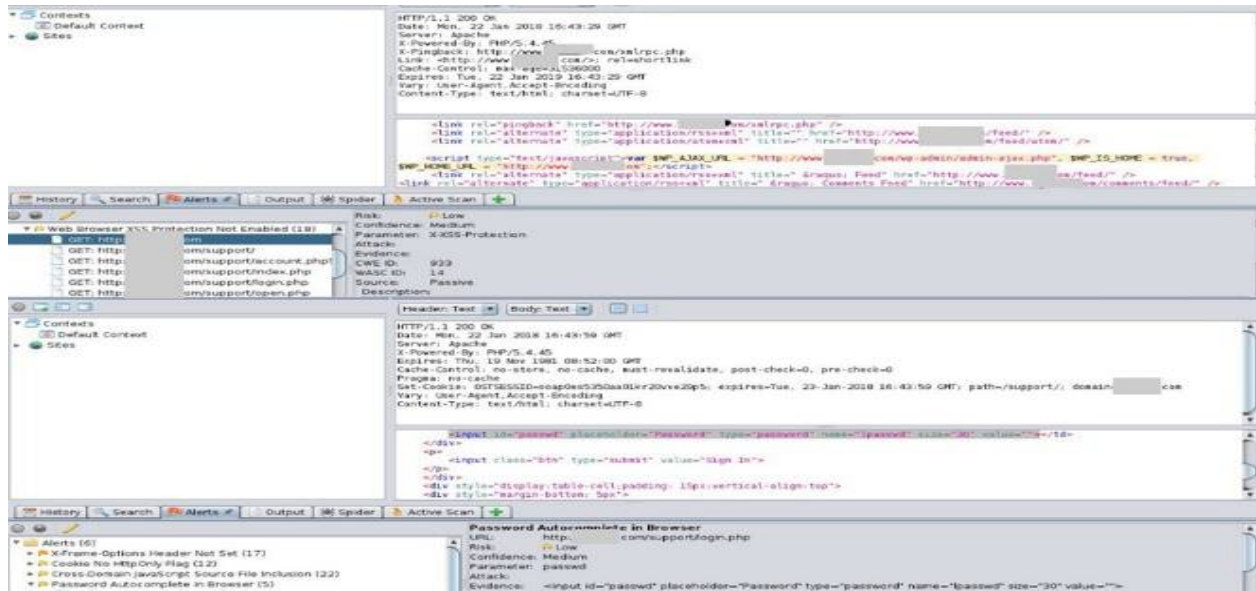


Fig.7 SECURITY MISCONFIGURATION FOUND

## VI.8 CROSS-SITE SCRIPTING (XSS)

Cross-site scripting is a most prevalent threat for web application. Cross-site scripting is an attack against a web application which exploit some vulnerability of it. There are many types of cross-site scripting such as reflected cross-site scripting, stored cross-site scripting, DOM cross-site scripting. In the advanced web penetration testing we found and successfully implement cross-site scripting on a web applications. The result of the cross-site scripting is showing below and demonstrate how cross-site scripting is effective.

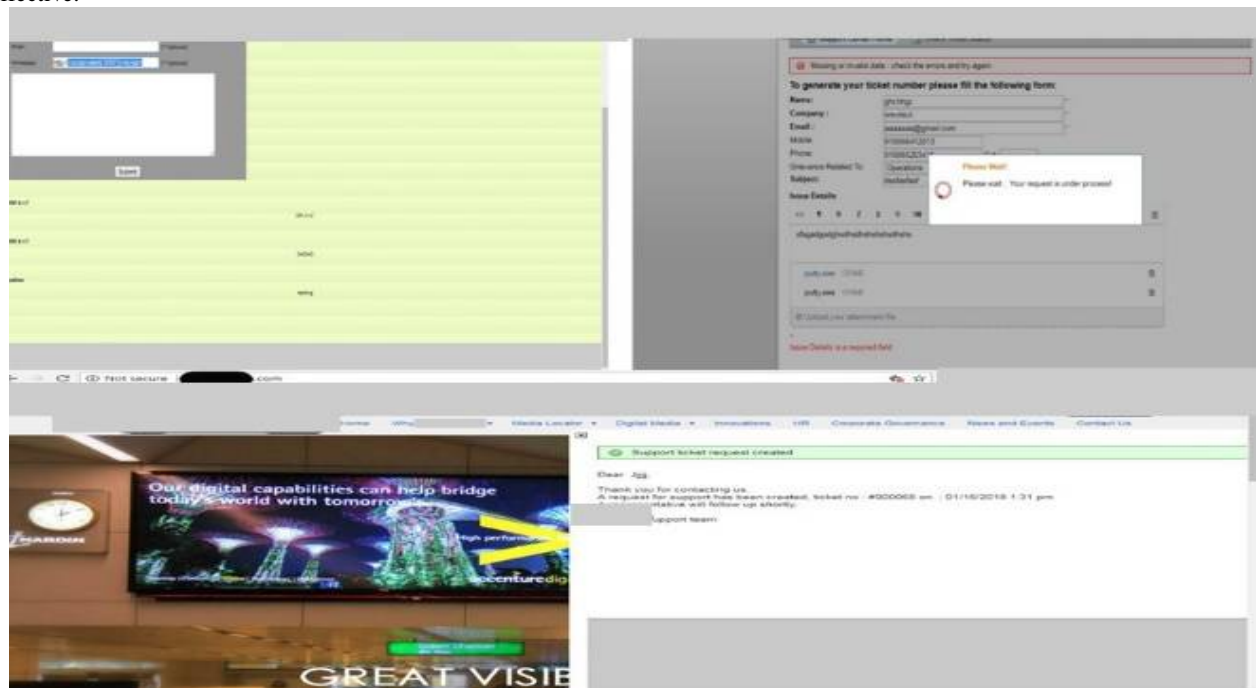


Fig.8 UPLOADED SCRIPT AND EXE FILE



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018

The cross-site scripting happen with a written script in the input field and reflected on the web application and the second was uploading an exe file (virus) into the web application.

## VI.9 INSECURE DESERIALIZATION

Insecure deserialization is a new threat and attacks which has been introduced in OWASP 2017. Insecure deserialization allow the attacker to access directory which supposed to not be index. As there are some html pages which should not be index, by using this attack discovery of source code and file can be possible. Serialization is a process of converting an object into a well-structured format which is non-volatile and those structured format can be send through network or using streams. So from the previous definition we can say that deserialization is the opposite of serialization. Serialization is well used in web application for XML and JSON file. Insecure deserialization is threat and attack in the sense that web application de serializing untrusted user input. To illustrate this attack we perform this attacks against web application and the result is shown below:

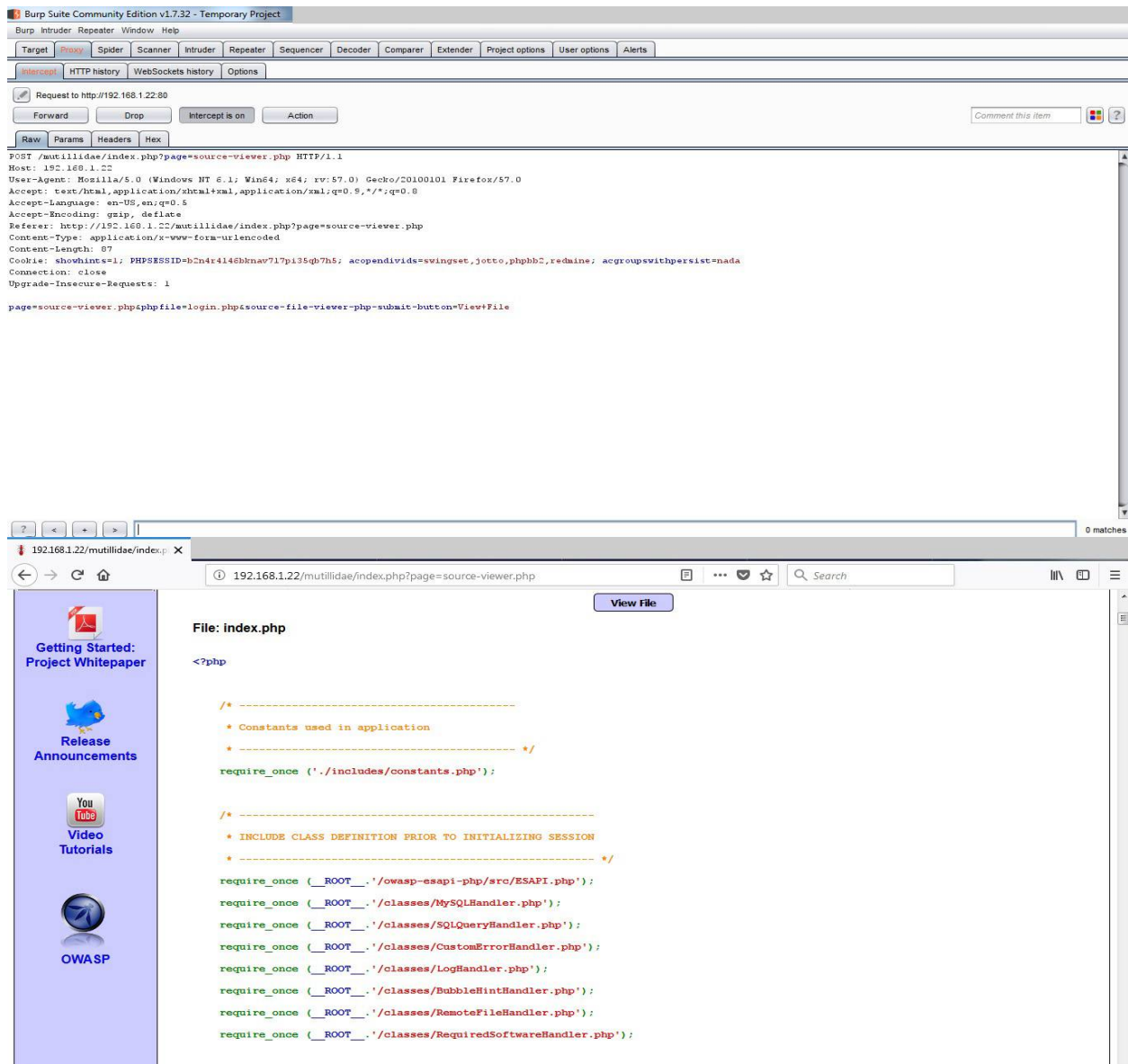


Fig.9 ACCESS RESTRICTED URL PAGE WITH INSECURE DESERIALIZATION



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018

## VI.10 USING COMPONENT WITH KNOWN VULNERABILITY

Component with known vulnerability is a threat for the web application in the sense that when a web application have many component some component might present many and serious vulnerability which can be exploited by the attacker. Some component known are for example windows server, WordPress module, windows xp and many other component from different technology. Know vulnerability can be exploited by using or developing some framework but as some framework already exist such metasploit some component used in web application have their exploit in metasploit where any attacker or unauthorized user can use to exploit the vulnerability. Even the international database call common vulnerability existent show the proper module available in metasploit to leverage the weakness.

CVE-ID	
<b>CVE-2017-8295</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
WordPress through 4.7.4 relies on the Host HTTP header for a password-reset e-mail message, which makes it easier for remote attackers to reset arbitrary passwords by making a crafted wp-login.php?action=lostpassword request and then arranging for this message to bounce or be resent, leading to transmission of the reset key to a mailbox on an attacker-controlled SMTP server. This is related to problematic use of the SERVER_NAME variable in wp-includes/pluggable.php in conjunction with the PHP mail function. Exploitation is not achievable in all cases because it requires at least one of the following: (1) the attacker can prevent the victim from receiving any e-mail messages for an extended period of time (such as 5 days), (2) the victim's e-mail system sends an autoresponse containing the original message, or (3) the victim manually composes a reply containing the original message.	

Fig.10 WORDPRESS VULNERABILITY

## VI.11 INSUFFICIENT LOGGING AND MONITORING

Insufficient logging and monitoring is the last threat for web application defined by OWASP. Every attack start by vulnerability probing means the attackers need to get into the system and try to find many vulnerability as possible. By doing this if the attacker is not being detected by the web application or by any means such as firewall or web application firewall or SIEM then we can conclude to a poor of logging and monitoring of the web application and developer.

## VII OWASP TOP TEN THREAT COUNTERMEASURES

- Sanitize user Input(Cross-site Scripting)
- Ensure all login, even login failure at the both side client and server side being monitor and able to detect suspicious activity(Insufficient logging and monitoring)
- Download official component from trusted sources(Using Component with known vulnerability)
- Enforcing strict constraint during deserialization(Insecure deserialization)
- Review and update the security configuration on regular basis( Security Misconfiguration)
- Invalidate the token once logout take place(Broken Authentication)
- Disable XML External Entities and DTD process in all XML used by the web application
- Encrypt all data with secure protocol such as TLS or HTTPS or SSL.(Sensitive data exposure)
- Implement weak password check with dictionary password and increase delay failed login attempts.
- Use positive white-list server side input(SQL Injection)

## VII. STEP TO SECURE WEB APPLICATIONS

**SECURE WEB APPLICATIONS PERIMETER:** use an iterative process to secure web application. Collection of 100% of traffic toward the web application to be able to analyze traffic and detect malicious activity within web application.

**TOOL SELECTION:** for securing web application, it is important to define which tools is necessary for different security categories such testing, scanning and protection. Having tools to secure your web application is not sufficient which is matter is where to deploy and proper strategies to secure web application

**DEFINE IMPLEMENTATION METRICS:** Without measurable statistics, it is difficult to determine when your organization has installed enough of



# International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018

the right security tools where needed having proper statistics of the code scanned is important which bring a great view of security for web application.

**SET AN IMPLEMENTATION DEADLINE AND CHECKPOINTS:** fixing a proper timing when the installations of tools have to start and end. Determine a periodic checkup, it will allow to determine if any checkup has been missed and will opportunity to get feedback from installed tools and allow to update the web application perimeter

**ANALYZE COLLECTED METRICS:** once the tools is installed, it generate logs, analyzing log and correlate each logs is a crucial task which help to identify the bad and goods events which occurred and allow to rectify certain configuration of the programs

## IX. FUTURE ADVANCEMENTS

The future work will be to reduce the false positive given by some web application scanner by writing some script which can be included in the web application scanner to reduce the false positive. Increasing the security level of web application is by secure the coding of the web application and our task will focus on secure component of web application, enhance authentication by new mechanism such as OTP or two factor authentication or behavioral mechanism.

## X. CONCLUSION

Advanced Penetration Testing is a good way and practice to not only get the security posture of the web application but it show the proof that vulnerability exist and exploit them as an attacker could have exploit. Penetration testing is a good test that every organization should perform to mitigate risk and avoiding losing crucial information. Providing advanced penetration testing to an organization is a best choice which will help mitigate and reduce the risk faced by web application when deploy or already existing. Advanced web penetration testing present man advantages which is finding more vulnerability than traditional penetration testing. Developer should now include security in all software developed to protect customer and organization asset, reducing the risk of being compromised at development is important for security.

## REFERENCES

- [1] OWASP Top Ten 2017 OWASP.ORG
- [2] WEB APPLICATION STATISTICS Q1 2017
- [3] CVEDETAILS.COM
- [4] Critical Analysis on Web Application Firewall Solutions (2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS) Abdul Razzaq, Ali Hur, Sidra Shahbaz, Muddassar Masood, H Farooq Ahmad School of Electrical Engineering and Computer Science (SECS)National University of Sciences and Technology, Islamabad, Pakistan)
- [5] VULNERABILITY ASSESSMENT AND PENETRATION TESTING Ankita Gupta, Kavita , Kirandeep Kaur Computer Science Department, PEC University of Technology, India Electronics and Electrical Communication Department, PEC University of Technology, India
- [6] UNDERSTANDING WEB APPLICATION SECURITY CHALLENGES, IBM 2008
- [7] [HTTPS://DOCS.KALI.ORG/INTRODUCTION/WHAT-IS-KALI-LINUX](https://docs.kali.org/introduction/what-is-kali-linux)
- [8] SANS Institute InfoSec Reading Room Getting Started with Web Application Security Written by Gregory Leonard February 2016 Sponsored by Veracode
- [9] Web Applications Security and Vulnerability Analysis Financial Web Applications Security Audit – A Case Study Tiago Vieira, Carlos Serrão School of Technology and Architecture ISCTE-IUL/ISTAR-IUL Lisbon, Portugal



ISSN(Online): 2320-9801  
ISSN (Print) : 2320-9798

# International Journal of Innovative Research in Computer and Communication Engineering

*(A High Impact Factor, Monthly, Peer Reviewed Journal)*

Website: [www.ijircce.com](http://www.ijircce.com)

Vol. 6, Issue 4, April 2018

## BIOGRAPHY



SUBARNA PANDA,  
M.Tech (CSE)  
Working as Ass. Professor Jain University Jayanagar, Bangalore  
Department Computer Science Information Technology



BOKOBRI LEKPELI KOISSY FRANCK OLIVIER  
Master Computer Application (information Security and Management Services)  
Cyber Security Analyst (Cisco)  
Worked at HKIT Security Solutions