

# Vulnerability Assessment & Penetration Test Report

OLYMPIC GOLD QUEST

Submitted by

Arrka



**Arrka**

Jan 2019

**Document Information:**

<b>Project Name:</b>	Vulnerability Assessment & Penetration Test Report
<b>Document Title:</b>	OLYMPIC GOLD QUEST VAPT Draft Report

**Document History:**

Version	Author	Date	Change Description
0.1	Arrka	17-Jan-2019	Draft Release

## Table of Contents

<b>1. INTRODUCTION</b>	<b>4</b>
<b>2. OBJECTIVE</b>	<b>4</b>
2.1. ASSESSMENT DURATION	4
<b>3. SCOPE</b>	<b>4</b>
<b>4. RISK CLASSIFICATION</b>	<b>5</b>
4.1. VULNERABILITY ASSESSMENT & PENETRATION TESTING	5
<b>5. EXECUTIVE SUMMARY</b>	<b>6</b>
5.1. TECHNICAL ISSUES	8
5.1.1. Security Vulnerability Summary	8
<b>6. OUR APPROACH TO CONDUCTING THE TESTS</b>	<b>9</b>
6.1. TESTS CONDUCTED	9
<b>7. DETAILED SYNOPSIS FOR SECURITY VULNERABILITIES</b>	<b>12</b>
7.1. CROSS SITE SCRIPTING (XSS)	12
7.2. TOO LONG OPTIONS PARAMETER	13
7.3. TELCONDEX SIMPLE WEBSERVER BUFFER OVERFLOW	13
7.4. FORMAT STRING ON HTTP METHOD NAME	14
7.5. BROWSEGATE HTTP HEADERS OVERFLOWS	14
7.6. WEBSPHERE EDGE CACHING PROXY DENIAL OF SERVICE	15
7.7. WEBLOGIC SERVER DOS	15
7.8. TRIPLE DES BIRTHDAY ATTACK VULNERABILITY (SWEET32)	16
7.9. SSL/TLS: DIFFIE-HELLMAN KEY EXCHANGE INSUFFICIENT DH GROUP STRENGTH VULNERABILITY	17
7.10. SSL/TLS WEAK CIPHER SUITE AND RC4 CIPHER SUITES SUPPORTED	20
7.11. SSH WEAK MAC ALGORITHMS SUPPORTED	21
7.12. TCP TIMESTAMPS	22
7.13. SENSITIVE INFORMATION DISCLOSURE	23
7.14. WEB BROWSER 'X-XSS-PROTECTION' NOT ENABLED	23
7.15. NO "SECURE" COOKIE ATTRIBUTE	24
7.16. NO 'HTTPONLY' COOKIE ATTRIBUTE	25
7.17. 'X-CONTENT-TYPE' HEADERS NOT SET	26
7.18. SYSTEM TESTED AND OPEN PORTS	27
<b>8. ABOUT ARRKA</b>	<b>28</b>
<b>9. LIMITATIONS ON DISCLOSURE AND USE OF THIS REPORT</b>	<b>29</b>
<b>10. APPENDIX</b>	<b>30</b>
10.1. REFERENCES	30

## 1. Introduction

The report document hereby describes the proceedings and results of the Assessment exercise conducted on the OLYMPIC GOLD QUEST Web Applications and Servers. OLYMPIC GOLD QUEST authorized the assessment team to perform the assessment exercise on their infrastructure to identify potential gaps and issues in their infrastructure. The report hereby enlists the findings and our recommendations.

## 2. Objective

The objective of the exercise was to assess the web applications and servers in its current state and provide an Assessment Report comprising remediation strategy and recommendations to help mitigate the identified findings and risks during the activity.

### 2.1. Assessment Duration

Start Date:	09-01-2019
End Date:	15-01-2019

## 3. Scope

The section defines the scope of assets / systems covered under assessment.




Websites
www.olympicgoldquest.com
www.olympicgoldquest.in
www.ogq.co.in

## 4. Risk Classification

### 4.1. Vulnerability Assessment & Penetration Testing

The final risk value of the finding identified is arrived at by considering the likelihood of occurrence of an issue by exploiting the vulnerability and its impact on OLYMPIC GOLD QUEST infrastructure.

Following is the risk classification:

<b>Low</b> 	<b>Medium</b> 	<b>High</b> 
The weakness identified has the potential of undermining the operations or provide infrastructure-related information which helps them in disrupting operations.	The weakness identified does not directly leads to downtime. However, the weakness may be used to gain sufficient information to bring the application down.	The weakness identified has the potential of directly compromising the integrity, and / or availability of the application.

## 5. Executive Summary

This document is a report of the vulnerability assessment & penetration testing exercise conducted by Arrka for OLYMPIC GOLD QUEST.

Vulnerability Assessment & Penetration testing is an authorized attempt to simulate the activities of a hacker and check whether security controls implemented on the target can be circumvented.

Arrka's Assessment team reviewed the application for adequacy of the existing controls in accordance with standard methodology and industry known best practices. A comprehensive security assessment exercise was performed by domain experts on the target application.

The Arrka team conducted various tests over a period via different tools (Burp Suite, OWASP ZAP, Retina Network Scanner, Nmap, OpenVAS and manual exploits) and found the infrastructure to be insecure.

The Arrka approach for the testing phase was also to identify weaknesses that are potentially exploitable and can result in loss of data as well as reputation. Some of the key weaknesses we were able to exploit, and we suspect others can exploit are:

- Obsolete software versions and in some cases, software being used. These are easily exploitable and have the tendency to be broken into easily.
- Encryption technology used has been broken and several exploits are available. This means data/information transmitted encrypted can also be stolen and de-crypted to access the same information in clear text.
- The server has several vulnerabilities which can be exploited, and an attacker can get in through multiple combinations.

We feel that OGQ should work to close on all the vulnerabilities and also set up monitoring systems so that we can get to know when someone is trying to probe us OR even attack. These systems will go a long way in mitigating threats as well as serving as alerting mechanisms to aid in prevention of attacks.

The following are our key observations from the Vulnerability Assessment & Penetration Testing exercise:

- Web application is vulnerable to Cross-Site Scripting (XSS) attack.
- The servers support weak Diffie-Hellman key strength.
- Servers are vulnerable to man-in-the-middle attacks like Triple DES Birthday Attack (Sweet32).
- The HTTP response headers lack basic security Headers and Attributes.
- Some Security Misconfigurations are present along with user data being sent in Unencrypted form.
- Many software used on the servers need an update to the latest version.

DRAFT

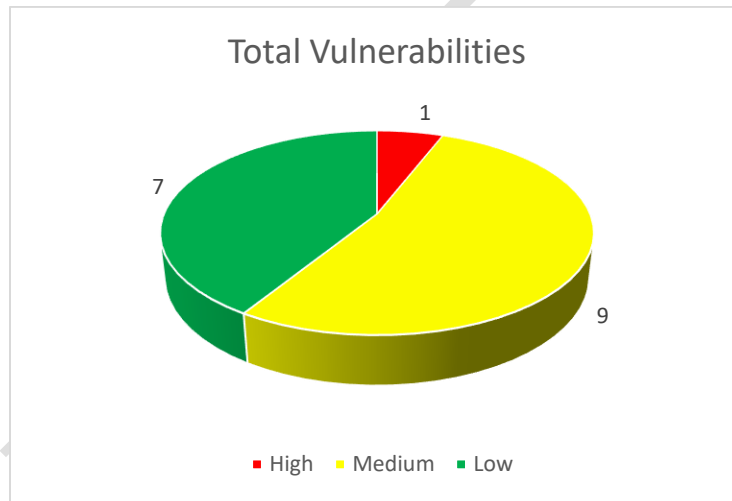
**5.1. Technical Issues**

The following table is the summary of findings, which summarizes the overall risks identified during the tests. For details, refer to section “Detailed Technical Summary”.

**5.1.1. Security Vulnerability Summary**

Total of 01 High, 09 Medium, and 07 Low risk issues were identified during the Assessment Exercise as presented below.

HIGH	MEDIUM	LOW
<b>01</b>	<b>09</b>	<b>07</b>





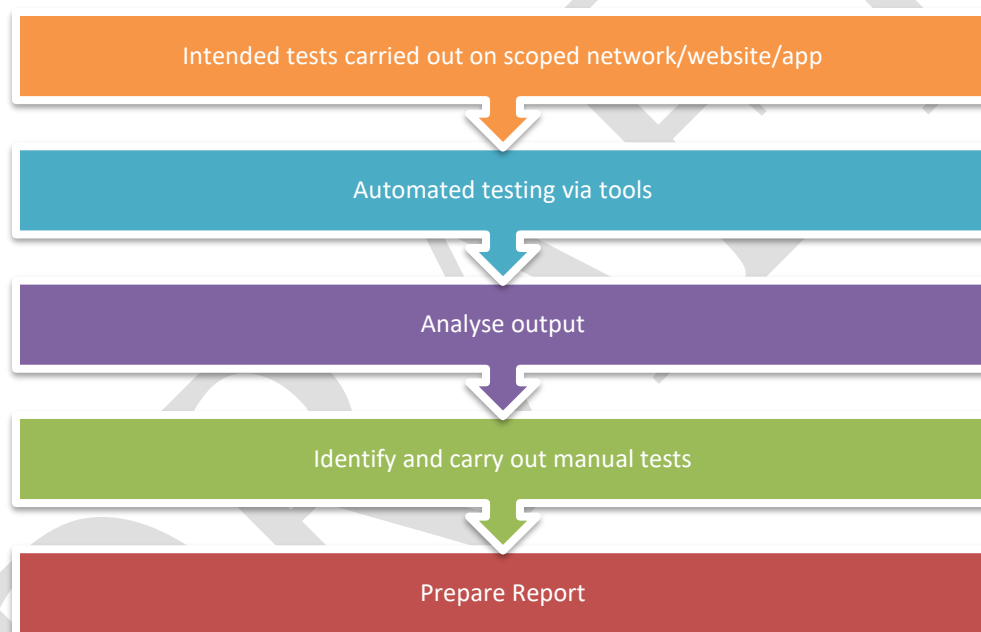
## 6. Our Approach to Conducting the Tests

Security testing (VA/PT) is an authorized attempt to simulate the activities of an attacker and

- check whether security controls implemented on the target can be circumvented and
- identify opportunities available to exploit target system vulnerabilities.

The security tester attempts to exploit the control weaknesses/ vulnerabilities to gain unauthorized access to the target system. We used the approach as described below:

### Approach and Methodology for Penetration Testing:



### 6.1. Tests Conducted

Primarily manual testing methods were used, and logs were captured, or the results were manually observed. This was done to mimic real life attackers, thus further increasing the accuracy of the results. As for automated tools, the logs captured were further explored by manual testing methods, applying years of experience and expertise.

Some of the tests conducted on the application in-scope were:

- Port Scan and Detection (Stealth/ Passive/ Active)
  - This is for identifying icmp filters on the perimeter and ports available for traffic. This includes checking for tcp and udp filters as well as using syn scans to walk through the perimeter.
- OS Detection
  - This is to guess the operating system of the target systems, which allows us to select vulnerabilities specific to the OS to be used for exploits.
- Service Identification
  - This is to guess the services running on the port. E.g. http service may be running on a port other than 80.
- Web Search for internal information
  - This is a check done across web sites and search engines. The idea is to see if someone has put details there which could give clues to the hidden areas/ vulnerabilities/ issues that can be exploited, of the applications/ infrastructure.
- Directory Traversal
  - Check on web sites to ensure directory cannot be browsed through and has been disabled.
- Software Misconfiguration (Security Controls)
  - Check for various configuration parameters which could allow access to the server/ data

## OLYMPIC GOLD QUEST VAPT Draft Report

- Insecure Cryptographic Transmission / Storage
  - Check for SSL key strength, SSL cipher and corresponding certificate related vulnerabilities.
- Internal Details Disclosure
  - Check for comments left over in the code/ pages which could reveal internal schema/ data locations.
- SMTP Relay
  - Check for relay enabled in the mail configuration by using commands to connect and send email from the outside without logging into the network.
- OWASP Top 10 2013:

Category	Attack Type
A1	Injection Attacks (SQL injections, Code injections)
A2	Broken Authentication and Session Management
A3	Cross Site Scripting (XSS)
A4	Insecure Direct Object References
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Missing Functional Level Access Control
A8	Cross Site Request Forgery (CSRF)
A9	Using Components with Known Vulnerabilities
A10	Invalidated Redirects and Forwards

## 7. Detailed Synopsis for Security Vulnerabilities

### 7.1. Cross Site Scripting (XSS)

Risk Rating	References
High <span style="display: inline-block; width: 50px; height: 10px; background-color: red; vertical-align: middle;"></span>	OWASP A3

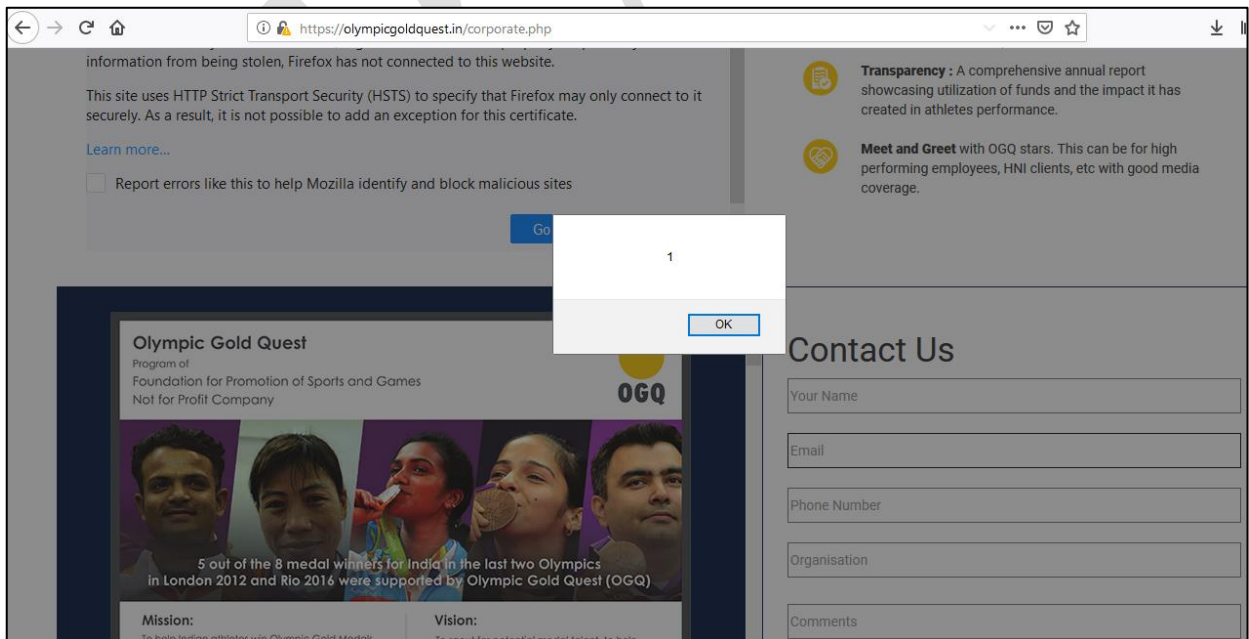
#### Our Observation:

Reflected Cross-site Scripting (XSS) occur when an attacker injects browser executable code within a single HTTP response. The injected attack is not stored within the application itself; it is non-persistent and only impacts users who open a maliciously crafted link or third-party web page. The attack string is included as part of the crafted URI or HTTP parameters, improperly processed by the application, and returned to the victim.

#### Altered Request:


```
<h2 class="">Contact Us</h2>
<form class="contact form" accept-charset="utf-8" id="contactForm" name="contactForm" method="post" action="corporate.php" autocomplete="off">
<input type="text" id="fullname" name="fullname" value="" placeholder="Your Name" class="textboxsize">
<br>
<br>
<input type="text" id="email" name="email" value="" onmouseover="alert(1);" placeholder="Email" class="textboxsize">
<br>
```

XSS successful.




<b>Affected Systems</b>
www.olympicgoldquest.in
<b>Suggested Mitigation</b>
Except for alphanumeric characters, escape all characters with the HTML Entity <code>&amp;#xHH;</code> format, including spaces. (HH = Hex Value)  Refer to: <a href="https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet">https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet</a>

### 7.2. Too long OPTIONS parameter


<b>Risk Rating</b>	<b>References</b>
Medium 	
<b>Our Observation:</b>	
It may be possible to make the web server crash or even execute arbitrary code by sending it a too long URL through the OPTIONS method.	
<b>Affected Systems</b>	
www.ogq.co.in	
<b>Suggested Mitigation</b>	
Upgrade the web server.	

### 7.3. TelCondex Simple Webserver Buffer Overflow


<b>Risk Rating</b>	<b>References</b>
Medium 	CVE-2003-1186
<b>Our Observation:</b>	
The TelCondex Simple Webserver is vulnerable to a remote executable buffer overflow, due to missing length check on the referrer-variable of the HTTP-header.	
<b>Affected Systems</b>	

www.ogq.co.in
<b>Suggested Mitigation</b>
Upgrade version 2.13 or later <a href="http://www.yourinfosystem.de/download/TcSimpleWebServer2000Setup.exe">http://www.yourinfosystem.de/download/TcSimpleWebServer2000Setup.exe</a>

#### 7.4. Format string on HTTP method name


Risk Rating	References
Medium 	
<b>Our Observation:</b>	
The remote web server seems to be vulnerable to a format string attack on the method name. An attacker might use this flaw to make it crash or even execute arbitrary code on this host.	
<b>Affected Systems</b>	
www.ogq.co.in	
<b>Suggested Mitigation</b>	
Upgrade your software or contact your vendor and inform him of this vulnerability	

#### 7.5. BrowseGate HTTP headers overflows

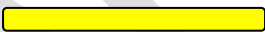
Risk Rating	References
Medium 	CVE-2000-0908
<b>Our Observation:</b>	
It was possible to kill the BrowseGate proxy by sending it an invalid request with too long HTTP headers (Authorization and Referrer) A cracker may exploit this vulnerability to make your web server crash continually or even execute arbitrary code on your system.	
<b>Affected Systems</b>	
www.ogq.co.in	

<b>Suggested Mitigation</b>
Upgrade your software or protect it with a filtering reverse proxy

**7.6. WebSphere Edge caching proxy denial of service**

<b>Risk Rating</b>	<b>References</b>
Medium 	CVE-2002-1169
<b>Our Observation:</b>	
We could crash the WebSphere Edge caching proxy by sending a bad request to the helpout.exe CGI.	
<b>Affected Systems</b>	
www.ogq.co.in	
<b>Suggested Mitigation</b>	
Upgrade your web server or remove this CGI.	

**7.7. WebLogic Server DoS**

<b>Risk Rating</b>	<b>References</b>
Medium 	CVE-2001-0098
<b>Our Observation:</b>	
Requesting an overly long URL starting with a double dot can crash certain version of WebLogic servers.	
<b>Affected Systems</b>	
www.ogq.co.in	
<b>Suggested Mitigation</b>	
Upgrade to at least WebLogic 5.1 with Service Pack 7	

### 7.8. Triple DES Birthday Attack Vulnerability (Sweet32)

Risk Rating	References
Medium <span style="background-color: yellow; border: 1px solid black; display: inline-block; width: 100px; height: 15px; vertical-align: middle;"></span>	CVE-2016-2183

**Our Observation:**

The Triple-DES cipher algorithm contains a vulnerability which can allow an attacker to recover secure HTTP cookies when performing a man-in-the-middle attack. During our assessment we observed this vulnerability in some servers.


```
Host is up (0.11s latency).
PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http Apache httpd
|_http-server-header: Apache
|_ssl-enum-ciphers:
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
```

```
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_ least strength: C
```



<b>Affected Systems</b>
www.olympicgoldquest.in
<b>Suggested Mitigation</b>
Disable Triple-DES Ciphers on the system

### 7.9. SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Risk Rating	References
Medium 	CVE-2014-3566, CVE-2014-8730

**Our Observation:**

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

```
Host is up (0.12s latency) .
Not shown: 974 filtered ports
PORT      STATE SERVICE
20/tcp    closed ftp-data
21/tcp    open  ftp
| ssl-dh-params:
|  VULNERABLE:
|  Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|  State: VULNERABLE
|  Transport Layer Security (TLS) services that use anonymous
|  Diffie-Hellman key exchange only provide protection against passive
|  eavesdropping, and are vulnerable to active man-in-the-middle attacks
|  which could completely compromise the confidentiality and integrity
|  of any data exchanged over the resulting session.
|  Check results:
|  ANONYMOUS DH GROUP 1
|  Cipher Suite: TLS_DH_anon_WITH_AES_256_GCM_SHA384
|  Modulus Type: Non-safe prime
|  Modulus Source: RFC5114/2048-bit DSA group with 256-bit prime order subgroup
|  Modulus Length: 2048
|  Generator Length: 2048
|  Public Key Length: 2048
|  References:
|  _ https://www.ietf.org/rfc/rfc2246.txt
22/tcp    open  ssh
25/tcp    open  smtp
26/tcp    closed rsftp
80/tcp    open  http
```

```

110/tcp  open  pop3
|  ssl-dh-params:
|  VULNERABLE:
|  Diffie-Hellman Key Exchange Insufficient Group Strength
|  State: VULNERABLE
|  Transport Layer Security (TLS) services that use Diffie-Hellman groups
|  of insufficient strength, especially those using one of a few commonly
|  shared groups, may be susceptible to passive eavesdropping attacks.
|  Check results:
|  WEAK DH GROUP 1
|      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
|      Modulus Type: Safe prime
|      Modulus Source: Unknown/Custom-generated
|      Modulus Length: 1024
|      Generator Length: 8
|      Public Key Length: 1024
|
|  References:
|  https://weakdh.org
143/tcp  open  imap
|  ssl-dh-params:
|  VULNERABLE:
|  Diffie-Hellman Key Exchange Insufficient Group Strength
|  State: VULNERABLE
|  Transport Layer Security (TLS) services that use Diffie-Hellman groups
|  of insufficient strength, especially those using one of a few commonly
|  shared groups, may be susceptible to passive eavesdropping attacks.
|  Check results:
|  WEAK DH GROUP 1
|      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
|      Modulus Type: Safe prime
|      Modulus Source: Unknown/Custom-generated
|      Modulus Length: 1024
|      Generator Length: 8
|      Public Key Length: 1024
|
|  References:
|  https://weakdh.org

```

```

443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
990/tcp  closed ftps
993/tcp  open  imaps
|  ssl-dh-params:
|  VULNERABLE:
|  Diffie-Hellman Key Exchange Insufficient Group Strength
|  State: VULNERABLE
|  Transport Layer Security (TLS) services that use Diffie-Hellman groups
|  of insufficient strength, especially those using one of a few commonly
|  shared groups, may be susceptible to passive eavesdropping attacks.
|  Check results:
|  WEAK DH GROUP 1
|      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
|      Modulus Type: Safe prime
|      Modulus Source: Unknown/Custom-generated
|      Modulus Length: 1024
|      Generator Length: 8
|      Public Key Length: 1024
|
|  References:
|  https://weakdh.org

```

```
995/tcp open pop3s
| ssl-dh-params:
| VULNERABLE:
| Diffie-Hellman Key Exchange Insufficient Group Strength
| State: VULNERABLE
| Transport Layer Security (TLS) services that use Diffie-Hellman groups
| of insufficient strength, especially those using one of a few commonly
| shared groups, may be susceptible to passive eavesdropping attacks.
| Check results:
| WEAK DH GROUP 1
| Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
| Modulus Type: Safe prime
| Modulus Source: Unknown/Custom-generated
| Modulus Length: 1024
| Generator Length: 8
| Public Key Length: 1024
| References:
|_ https://weakdh.org
1248/tcp open hermes
3306/tcp open mysql
50000/tcp closed ibm-db2
50001/tcp closed unknown
50002/tcp closed iiimf
50003/tcp closed unknown
50006/tcp closed unknown
50300/tcp closed unknown
50389/tcp closed unknown
50500/tcp closed unknown
50636/tcp closed unknown
50800/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 67.31 seconds
```

### Affected Systems

www.olympicgoldquest.in

### Suggested Mitigation

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group. (see <https://weakdh.org/sysadmin.html>).

For Apache Web Servers: Beginning with version 2.4.7, mod\_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

### 7.10. SSL/TLS Weak Cipher Suite and RC4 Cipher Suites Supported

Risk Rating	References
Medium <span style="display: inline-block; width: 100px; height: 10px; background-color: yellow; vertical-align: middle;"></span>	CVE-2015-2808, CVE-2013-2566

**Our Observation:**


A targeted SSL service that supports cryptographically weak cipher suites has been detected. An attacker may be able to leverage weaknesses in the encryption ciphers to gain access to sensitive information.

```
Host is up (0.11s latency).
PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http Apache httpd
|_http-server-header: Apache
|_ssl-enum-ciphers:
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
```


```
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 2048) - C
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_ least strength: C
```

<b>Affected Systems</b>
www.olympicgoldquest.in
<b>Suggested Mitigation</b>
Reconfigure the affected application to use a high-grade cipher suite and if possible, disable the use of RC4 ciphers in the application or its host operating system.


**7.11. SSH Weak MAC Algorithms Supported**

<b>Risk Rating</b>	<b>References</b>
Low 	
<b>Our Observation:</b>	
<p>The remote SSH server is configured to allow weak MD5 and/or 96-bit MAC algorithms.</p> <p>The following weak client-to-server MAC algorithms are supported by the remote service:</p> <ul style="list-style-type: none"> <li>• hmac-md5</li> <li>• hmac-md5-96</li> <li>• hmac-sha1-96</li> </ul> <p>The following weak server-to-client MAC algorithms are supported by the remote service:</p> <ul style="list-style-type: none"> <li>• hmac-md5</li> <li>• hmac-md5-96</li> <li>• hmac-sha1-96</li> </ul>	
<b>Affected Systems</b>	
www.olympicgoldquest.in	
<b>Suggested Mitigation</b>	
Disable the weak MAC algorithms.	


7.12. TCP Timestamps

Risk Rating	References
Low 	
<b>Our Observation:</b>	
<p>The remote host implements TCP timestamps and therefore allows to compute the uptime. It was detected that the host implements RFC1323.</p> <p>The following timestamps were retrieved with a delay of 1 seconds in-between:</p> <p>Packet 1: 1481034691</p> <p>Packet 2: 1481035837</p>	
<b>Affected Systems</b>	
www.olympicgoldquest.in, www.olympicgolquest.com, www.ogq.co.in	
<b>Suggested Mitigation</b>	
<p>To disable TCP timestamps on Linux, add the line <u>'net.ipv4.tcp_timestamps = 0'</u> to <i>/etc/sysctl.conf</i>. Execute <u>'sysctl -p'</u> to apply the settings at runtime.</p> <p>To disable TCP timestamps on Windows, execute <u>'netsh int tcp set global timestamps=disabled'</u></p> <p>Starting with Windows Server 2008 and Vista, the timestamp cannot be completely disabled. The default behaviour of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.</p> <p>See also: <a href="http://www.microsoft.com/en-us/download/details.aspx?id=9152">http://www.microsoft.com/en-us/download/details.aspx?id=9152</a></p>	

### 7.13. Sensitive Information Disclosure

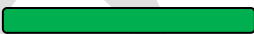
Risk Rating	References								
Low 									
<b>Our Observation:</b>									
In our assessment we noticed that user information was being transmitted in plain text.									
<table border="1"> <thead> <tr> <th>Raw</th> <th>Params</th> <th>Headers</th> <th>Hex</th> </tr> </thead> <tbody> <tr> <td colspan="4"> <pre>POST /corporate.php HTTP/1.1 Host: olympicgoldquest.in User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://olympicgoldquest.in/corporate.php Content-Type: application/x-www-form-urlencoded Content-Length: 164 Connection: close Cookie: _ga=GAL.2.1411555384.1547153010; _gid=GAL.2.256791555.1547537688; PHPSESSID=06a9s87i72g84n7b0vho2ahjr3 Upgrade-Insecure-Requests: 1  fullName=Rohitashwa+Singh&amp;email=rohitashwa.singh@40arrka.com&amp;phoneNumber=7409000989&amp;organisation=Arrka+Infosec&amp;message=Hello+world&amp;hiddenRecaptcha=&amp;senddata=sendnow</pre> </td> </tr> </tbody> </table>		Raw	Params	Headers	Hex	<pre>POST /corporate.php HTTP/1.1 Host: olympicgoldquest.in User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://olympicgoldquest.in/corporate.php Content-Type: application/x-www-form-urlencoded Content-Length: 164 Connection: close Cookie: _ga=GAL.2.1411555384.1547153010; _gid=GAL.2.256791555.1547537688; PHPSESSID=06a9s87i72g84n7b0vho2ahjr3 Upgrade-Insecure-Requests: 1  fullName=Rohitashwa+Singh&amp;email=rohitashwa.singh@40arrka.com&amp;phoneNumber=7409000989&amp;organisation=Arrka+Infosec&amp;message=Hello+world&amp;hiddenRecaptcha=&amp;senddata=sendnow</pre>			
Raw	Params	Headers	Hex						
<pre>POST /corporate.php HTTP/1.1 Host: olympicgoldquest.in User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://olympicgoldquest.in/corporate.php Content-Type: application/x-www-form-urlencoded Content-Length: 164 Connection: close Cookie: _ga=GAL.2.1411555384.1547153010; _gid=GAL.2.256791555.1547537688; PHPSESSID=06a9s87i72g84n7b0vho2ahjr3 Upgrade-Insecure-Requests: 1  fullName=Rohitashwa+Singh&amp;email=rohitashwa.singh@40arrka.com&amp;phoneNumber=7409000989&amp;organisation=Arrka+Infosec&amp;message=Hello+world&amp;hiddenRecaptcha=&amp;senddata=sendnow</pre>									
<b>Affected Systems</b>									
www.olympicgoldquest.in									
<b>Suggested Mitigation</b>									
User information must be encrypted or encoded before transmission.									

### 7.14. Web Browser 'X-XSS-Protection' Not enabled

Risk Rating	References
Low 	
<b>Our Observation:</b>	
Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server	

<pre>HTTP/1.1 200 OK Date: Thu, 10 Jan 2019 08:56:56 GMT Server: Apache X-Powered-By: PHP/5.5.38 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=m2ug21evc68308klo65h91soa3; path=/ Vary: Accept-Encoding,User-Agent X-FRAME-OPTIONS: SAMEORIGIN Content-Type: text/html</pre>
<b>Affected Systems</b>
www.olympicgoldquest.in
<b>Suggested Mitigation</b>
Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.


**7.15. No “secure” cookie Attribute**

Risk Rating	References
<b>Low</b> 	
<b>Our Observation:</b>	
<p>A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page, then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.</p>	
<pre>HTTP/1.1 200 OK Date: Thu, 10 Jan 2019 08:56:56 GMT Server: Apache X-Powered-By: PHP/5.5.38 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=m2ug21evc68308klo65h91soa3; path=/ Vary: Accept-Encoding,User-Agent X-FRAME-OPTIONS: SAMEORIGIN Content-Type: text/html</pre>	




<b>Affected Systems</b>
www.olympicgoldquest.in
<b>Suggested Mitigation</b>
Set the 'httpOnly' attribute for any session cookie.

**7.16. No 'HttpOnly' Cookie Attribute**

<b>Risk Rating</b>	<b>References</b>
Low 	
<b>Our Observation:</b>	
<p>A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page, then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.</p>	
<pre> HTTP/1.1 200 OK Date: Thu, 10 Jan 2019 08:56:56 GMT Server: Apache X-Powered-By: PHP/5.5.38 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=m2ug21evc68308klo65h91soa3; path=/ Vary: Accept-Encoding,User-Agent X-FRAME-OPTIONS: SAMEORIGIN Content-Type: text/html                     </pre>	
<b>Affected Systems</b>	
www.olympicgoldquest.com	
<b>Suggested Mitigation</b>	
Set the 'httpOnly' attribute for any session cookie.	

7.17. 'X-content-type' headers not set

Risk Rating	References
Low 	
<b>Our Observation:</b>	
<p>The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.</p> <pre data-bbox="402 737 1240 1094" style="border: 1px solid black; padding: 5px;"> HTTP/1.1 200 OK Date: Thu, 10 Jan 2019 08:56:56 GMT Server: Apache X-Powered-By: PHP/5.5.38 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-cache, must-revalidate Pragma: no-cache Set-Cookie: PHPSESSID=m2ug21evc68308k1o65h91soa3; path=/ Vary: Accept-Encoding,User-Agent X-FRAME-OPTIONS: SAMEORIGIN Content-Type: text/html                     </pre>	
<b>Affected Systems</b>	
www.olympicgoldquest.in	
<b>Suggested Mitigation</b>	
<p>Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.</p> <p>If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.</p>	

7.18. System Tested and Open Ports

Sr. No.	Application	Open Ports
1	www.olympicgoldquest.in	<ul style="list-style-type: none"> <li>• 21/tcp open ftp Pure-FTPd</li> <li>• 22/tcp open ssh OpenSSH 5.3 (protocol 2.0)</li> <li>• 25/tcp open smtp?</li> <li>• 80/tcp open http Apache httpd</li> <li>• 110/tcp open pop3 Dovecot pop3d</li> <li>• 143/tcp open imap Dovecot imapd</li> <li>• 443/tcp open ssl/https Apache</li> <li>• 465/tcp open ssl/smtp Exim smtpd 4.91</li> <li>• 587/tcp open smtp Exim smtpd 4.91</li> <li>• 993/tcp open ssl/imap Dovecot imapd</li> <li>• 995/tcp open ssl/pop3 Dovecot pop3d</li> <li>• 1248/tcp open hermes?</li> </ul>
2	www.olympicgoldquest.com	<ul style="list-style-type: none"> <li>• 80/tcp open http</li> <li>• 2000/tcp open tcpwrapped</li> <li>• 8008/tcp open tcpwrapped</li> </ul>
3	www.ogq.co.in	<ul style="list-style-type: none"> <li>• 80/tcp open tcpwrapped</li> <li>• 8008/tcp open http Fortinet FortiGuard block page</li> </ul>

## 8. About Arrka

Arrka Consulting provides consulting, advisory & testing services in the Information Risk domain. We specialize in Cybersecurity, Information Security and Data Privacy.

Arrka has a specialized offering – the ArrkaCISO service – developed specifically for Small & Mid-Sized companies. Here we function as the extended CISO arm of the organization, helping the organization understand its information risks; implement a formal program to mitigate and manage them; and to help them do this on a sustained basis by taking on the maintenance, management and upgradation of the program on an on-going basis. We also run a specialized Security Testing Lab from where we carry out specialized security tests like VA/PT.

In the Data Privacy domain, we are one of the pioneers in India. We help organizations implement and manage privacy programs. We have done this for very large organizations as well as small companies who deal with sensitive personal data.

Arrka has also set up a specialized Privacy Testing Lab – the first of its kind in India – that exclusively does privacy testing.

## 9. Limitations on Disclosure and Use of this Report

This report contains sensitive and confidential information about the infrastructure and controls framework designed and implemented for OLYMPIC GOLD QUEST.

The report also highlights certain controls weaknesses identified during the review carried out by Arrka. Therefore, the information contained in this report can be maliciously used to exploit the issues reported in the present installation and configuration. We, therefore, strongly recommend OLYMPIC GOLD QUEST treat this report as 'classified' information, restrict its circulation, and control the process of making additional copies thereof. The distribution of this report should be limited to concerned and appropriate officials only.

The report is intended for internal use only and should not be forwarded to any third party/customer of OLYMPIC GOLD QUEST. This report is issued to inform the OLYMPIC GOLD QUEST management of potential weaknesses and risks in the web and mobile applications found by the Arrka Team and should not be used for any other purpose. The use of our reports for taking business decisions including decisions of strategic, financial, economic or marketing nature will be at your own risk.

## 10. Appendix

### 10.1. References

- OSSTMM  
<http://www.osstmm.org>
- OWASP  
<http://www.owasp.org>
- OSVDB  
<http://osvdb.org/>
- CWE  
<http://cve.mitre.org/>  
<http://cwe.mitre.org/>

**End of Document**