Vulnerability Assessment and Penetration Testing

Sample Report

Disclaimer

Attention: This document contains information from "***Company Name***" that is confidential and privileged. This information is intended for the private use of the company. By accepting this document, you agree to keep the contents in confidence and not to copy them, disclose or distribute this without a written confirmation from "***Company Name***". If you are not the intended recipient, be aware that any disclosure, copying or distribution of the contents of this document is strictly prohibited and can lead to legal actions.

Note: We are not using any kind of automation tools for this testing. We visited every link manually as an external user and tried to find out critical & high-level vulnerabilities.

VAPT SCAN REPORT SUMMARY

TARGET URL	https://www.[redacted].org/
SCAN DATE	04-01-2020 14:48:08 (UTC+05:30)
REPORT DATE	31-01-2020 10:09:49
SCAN DURATION	02:01:46
TESTER NAME	Hrithik Lall (CCNA, CEH V10, C|NPT)

SCAN SETTINGS

ENABLED ENGINES	SQL Injection, SQL Injection (Boolean), SQL Injection (Blind), Cross-site Scripting, Command Injection, Command Injection (Blind), Local File Inclusion, Remote File Inclusion, Code Evaluation, Server-Side Template Injection, HTTP Header Injection, Open Redirection, Expression Language Injection, Web App Fingerprint, RoR Code Execution, WebDAV, Reflected File Download, Insecure Reflected Content, XML External Entity, File Upload, Windows Short Filename, Cross-Origin Resource Sharing (CORS), HTTP Methods, Server-Side Request Forgery (Pattern Based), Server-Side Request Forgery (DNS), SQL Injection (Out of Band), XML External Entity (Out of Band), Cross-site Scripting (Blind), Remote File Inclusion (Out of Band), Code Evaluation (Out of Band)
URL REWRITE MODE	Heuristic
DETECTED URL REWRITE RULES	None
EXCLUDED URL PATTERNS	(log|sign)\-?(out|off) exit endsession gtm\.js WebResource\.axd ScriptResource\.axd

VULNERABILITIES SUMMARY

CATEGORIES	ISSUES	INSTANCES	CONFIRMED
CRITICAL	0	0	0
HIGH	0	0	0
MEDIUM	2	2	2
LOW	0	0	0
INFORMATION	0	0	0
TOTAL	2	2	2

Table of Content

URL	Parameter	Method	Vulnerability	Confirmed
https://www.[redacted].org/		GET	Out-of-date Version (jQuery)	Yes
https://www.[redacted].org/		GET	[Possible] Internal IP Address Disclosure	Yes

1. Out-of-date Version (jQuery)

Identified the target web site is using jQuery and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of jQuery to the latest stable version.

Remedy References

Downloading jQuery

Known Vulnerabilities in this Version

Selector interpreted as HTML

Exploit

https://bugs.jquery.com/ticket/11290

Classification

OWASP 2013-A9 OWASP 2017-A9 PCI V3.1-6.2 PCI V3.2-6.2 CAPEC-310

Effected Url - https://www.[redacted].org/

Identified Version

1.8.2 (contains 1 medium vulnerabilities)

Latest Version

3.3.1

Vulnerability Database

Result is based on 26-04-2018 vulnerability database content.

Proof of Concept (POC): -

Request: -

Request

```
GET / HTTP/1.1
Host: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36
```

Response: -

Response

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache
Connection: Upgrade, Keep-Alive
Keep-Alive: timeout=5, max=75
Content-Type: text/html
Content-Encoding:
Upgrade: h2,h2c
Date: Sat, 04 Jan 2020 09:18:03 GMT
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href='http://fonts.googleapis.com/css?family=PT+Sans:400,700' rel='stylesheet' type='text/css'>
<link href="css/style.css" type="text/css" rel="stylesheet" />
<link rel="stylesheet" href="css/menu.css" type="text/css" media="screen" />
<link rel="stylesheet" href="css/demo.css">
<link rel="stylesheet" type="text/css" href="css/tabber.css" />
<link rel="stylesheet" href="css/jquery.mCustomScrollbar.css">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="Keywords" content="" />
<title>%ESU</title>
<style type="text/css">
<!--
.style1 {color: #1F34F5}
-->
</style>
</head>
<body>
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-133279703-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());

gtag('config', 'UA-133279703-1');
</script><script>
function myFunction() {
var myWindow = window.open("campus.php", "Campus", "toolbar=yes, scrollbars=yes, resizable=yes, top=200, left=200, width=1200, height=600");

}
</script>
<div class="header-wrapper">
<div class="inner-wrapper">
<div class="logo"><a href="index.php"><img src="images/logo.jpg" alt="" /></a></div>
<div class="header-menu">
<ul id="nav1">
<li><a href="admission.php">Admission</a>
<ul>
<li><a href="notice-adm.php">Notice</a></li>
<li><a hre
-
```

2. Active Mixed Content over HTTPS

Detected that an active content loaded over HTTP within an HTTPS page.

Impact

Active Content is a resource which can run in the context of your page and moreover can alter the entire page. If the HTTPS page includes active content like scripts or stylesheets retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

A man-in-the-middle attacker can intercept the request for the HTTP content and also rewrite the response to include malicious codes. Malicious active content can steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

Remedy

There are two technologies to defense against the mixed content issues:

1. HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page)
2. Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites.
3. Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example:

A protocol relative URL to load an style would look like <link rel="stylesheet" href="//example.com/style.css"/>.

Same for scripts <script type="text/javascript" src="//example.com/code.js"></script>

The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

External References

Mixed Content

Remedy References

- Wikipedia - HTTP Strict Transport Security
- Wikipedia - Content Security Policy

Classification

OWASP 2013-A6 OWASP 2017-A3 CWE-319

Effected Url - https://www.[redacted].org/cgi-sys/js/

Resources Loaded from Insecure Origin (HTTP)

http://fonts.googleapis.com/css?family=PT+Sans:400,700

Proof of Concept (POC): -

Request: -

Response: -

Response

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Server: Apache
Connection: Upgrade, Keep-Alive
Keep-Alive: timeout=5, max=75
Content-Type: text/html
Content-Encoding:
Upgrade: h2,h2c
Date: Sat, 04 Jan 2020 09:18:03 GMT
Vary: Accept-Encoding,User-Agent

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link href="http://fonts.googleapis.com/css?family=PT+Sans:400,700" rel="stylesheet" type="text/css">
<link href="css/style.css" type="text/css" rel="stylesheet" />
<link rel="stylesheet" href="css/menu.css" type="text/css" media="screen" />
<link rel="stylesheet" href="css/demo.css">
<link rel="stylesheet" type="text/css" href="css/tabber.css" />
<link rel="stylesheet" href="css/jquery.mCustomScrollbar.css">
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="description" content="" />
<meta name="keywords" content="" />
<title>BSUk</title>
<style type="text/css">
<!--
.style1 {color: #1F14F5}
-->
</style>
</head>
<body>
<!-- Global site tag (gtag.js) - Google Analytics -->
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-133279703-1"></script>
<script>
window.dataLayer = window.dataLayer || [];
function gtag(){dataLayer.push(arguments);}
gtag('js', new Date());

gtag('config', 'UA-133279703-1');
</script><script>
function myFunction() {
var myWindow = window.open("campus.php", "Campus", "toolbar=yes, scrollbars=yes, resizable=yes, top=100, left=200, width=1200, height=600");

}
</script>
<div class="header-wrapper">
<div class="inner-wrapper">
<div class="logo"><a href="index.php"><img src="images/logo.jpg" alt="" /></a></div>
<div class="header-menu">
<ul id="nav1">
<li><a href="admission.php">Admissions</a>
<ul>
<li><a href="notice-adm.php">Notice</a></li>
<li><a hre
-
```

Company Profile

Company Name: -

IEMA Research & Development Private Limited

Locations: -

- **India** - 601, Godrej Genesis Building, Block EP & GP, Kolkata - 700091, West Bengal, India.
- **Canada** - SAT Ventures Limited, Canada 404 - 6595 Bonsor Avenue, Burnaby, BC V5H4G5.

Contact Details: -

- **Email** - iema@iemlabs.com.
- **Phone**: **India**: +91 9163198148 | **Canada**: +1-604-431-979

Testing Date - 6th September, 2017

Tester Details: -

Name - Hrithik Lall

Designation - Chief Technical Officer (CTO)

Qualification - CCNA, CEH V10, ECSA V10, C|NPT