INFORMATION ASSURANCE AND AUDITING

IE 4040

Mini Project Report

Gunasekara K. G. P

B.Sc. (Hons) Degree in Information Technology specializing in Computer Systems & Network Engineering

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology

Sri Lanka

May 2020

DECLARATION

This is my own work and has not been submitted previously for a degree at this or any other university/institute.

To the best of my knowledge, it does not contain any material published or written by another person, except as acknowledged in the text.

Name	IT Number	Date
Gunasekara K.G.P	IT16085190	11/05/2020

ABSTRACT

The world is most reliant on the Internet. Nowadays, web security is the biggest challenge in the corporate world. It is considered as the principal framework for the worldwide data society. Web applications are prone to security attacks. Web security is securing a web application layer from attacks by unauthorized users. A lot of the issues that occur over a web application is mainly due to the improper input provided by the client. This paper discusses the different aspects of web security, and it's weakness. The main elements of web security techniques, such as passwords, encryption, authentication, and integrity, are also discussed in this paper. The anatomy of a web application attack and the attack techniques are also covered in detail. This paper explores several methods for combatting this class of threats and assesses why they have not proven more successful. This paper proposes a better way of minimizing this type of web vulnerabilities. It also provides the best security mechanisms for the said attacks.

TABLE OF CONTENTS

INFORMATION ASSURANCE AND AUDITING

IE 4040

Mini Project Report

B.Sc. (Hons) Degree in Information Technology specializing in Computer Systems & Network Engineering

Department of Computer Systems Engineering

Sri Lanka Institute of Information Technology
Sri Lanka

May 2020

1. INTRODUCTION

Software security testing is the process of assessing and testing a system to discover security risks and vulnerabilities of the system and its data. There is no universal terminology, but for our purposes, we define assessments as the analysis and discovery of vulnerabilities without attempting to exploit those vulnerabilities. We define testing as the discovery and attempted exploitation of vulnerabilities.

Security testing is often broken out, somewhat arbitrarily, according to either the type of vulnerability being tested or the type of testing being done. A common thing is,

- Vulnerability Assessment – The system is scanned and analyzed for security issues.
- Penetration Testing – The system undergoes analysis and attack from simulated malicious attackers.
- Runtime Testing – The system undergoes analysis and security testing from an end-user.
- Code Review – The system code undergoes a detailed review and analysis, looking specifically for security vulnerabilities.

Note that risk assessment, which is commonly listed as part of security testing, is not included in this list. That is because a risk assessment is not actually a test but rather the analysis of the perceived severity of different risks (software security, personnel security, hardware security, etc.) and any mitigation steps for those risks.

2. Tools for Web application testing

Top 10 Testing Automation Tools for Web application Testing.

- Selenium

  Selenium is a testing framework to perform web application testing across various browsers and platforms like Windows, Mac, and Linux. Selenium helps the testers to write tests in different programming languages like Java, PHP, C#, Python, Groovy, Ruby, and Perl. It offers a record and playback feature to write tests without learning Selenium IDE.

- TestingWhiz

  TestingWhiz is a test automation tool with the code-less scripting by Cygnet Infotech, a CMMi Level 3 IT solutions provider. TestingWhiz tool's Enterprise edition offers a complete package of various automated testing solutions like web testing, software testing, database testing, API testing, mobile app testing, regression test suite maintenance, optimization, and automation, and cross-browser testing.

- HPE Unified Functional Testing (HP – UFT formerly QTP)

  HP QuickTest Professional was renamed to HPE Unified Functional Testing. HPE UFT offers testing automation for functional and regression testing for software applications.Visual Basic Scripting Edition scripting language is used by this tool to register the test processes and operates the various objects and controls in testing the applications.

- TestComplete

  TestComplete is a functional testing platform that offers various solutions to automate testing for desktop, web, and

	mobile applications by SmartBear Software.
• Ranorex	anorex Studio offers various testing automation tools that cover testing all desktop, web, and mobile applications.
• Sahi	Sahi is a testing automation tool to automate web applications testing. The open-source Sahi is written in Java and JavaScript programming languages.
• Watir	Watir is an open-source testing tool made up of Ruby libraries to automate web application testing. It is pronounced as “water.”
• Tosca Testsuite	Tosca Testsuite by Tricentis uses model-based test automation to automate software testing.
• Telerik TestStudio	Telerik TestStudio offers one solution to automate desktop, web, and mobile application testing including UI, load, and performance testing.
• Katalon Studio	Katalon Studio is a free automation testing solution developed by Katalon LLC. The software is built on top of the open-source automation frameworks Selenium, Appium with a specialized IDE interface for API, web and mobile testing. This tool includes a full package of powerful features that help overcome common challenges in web UI test automation.

3. Introduction to “ZAP” penetration testing tool

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is explicitly designed for testing web applications and is both flexible and extensible.

At its core, ZAP is what is known as a “man-in-the-middle proxy.” It stands between the tester’s browser and the web application so that it can intercept and inspect messages sent between the browser and web application, modify the contents if needed, and then forward those packets on to the destination. It can be used as a stand-alone application and as a daemon process.

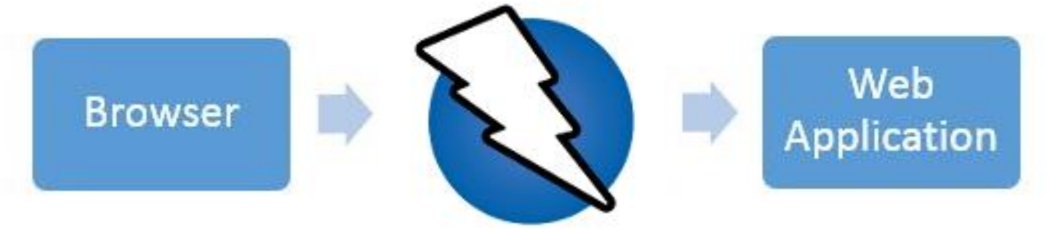


Fig 3.1

If there is another network proxy already in use, as in many corporate environments, ZAP can be configured to connect to that proxy.

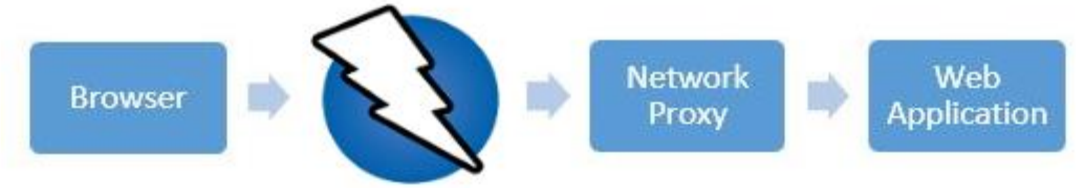


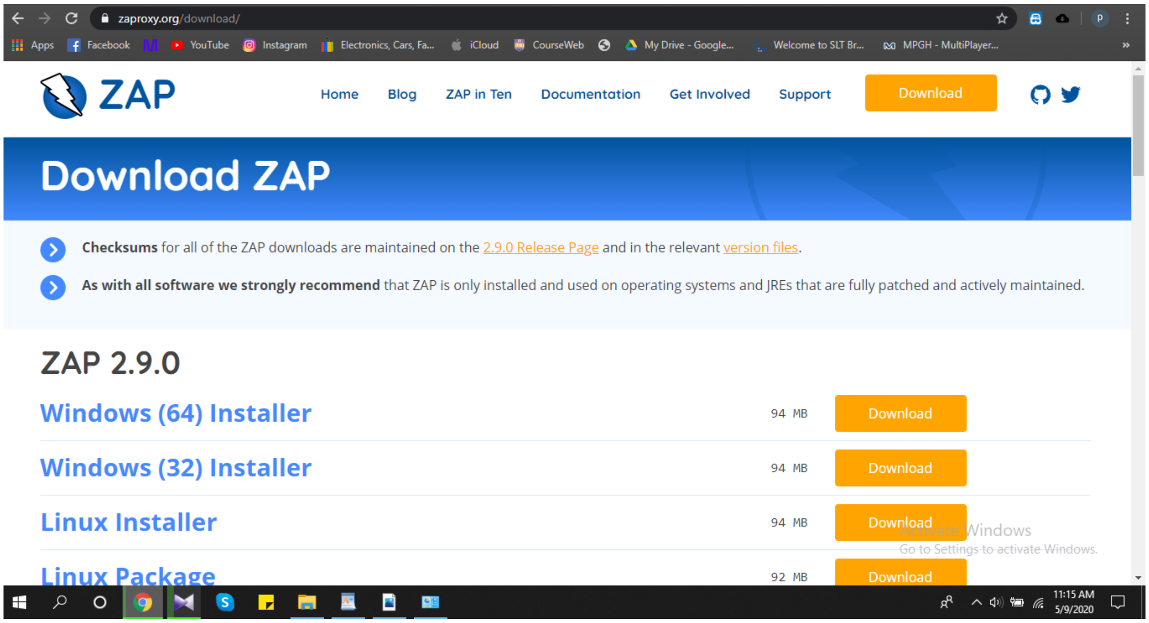
Fig 3.2

ZAP provides functionality for a range of skill levels – from developers, to testers new to security testing, to security testing specialists. ZAP has versions for each major OS and Docker, so you are not tied to a single OS. Additional functionality is freely available from a variety of add-ons in the ZAP Marketplace, accessible from within the ZAP client.

Because ZAP is open-source, the source code can be examined to see exactly how the functionality is implemented. Anyone can volunteer to work on ZAP, fix bugs, add features, create pull requests to pull fixes into the project, and author add-ons to support specialized situations.

4. Steps of auditing web application using “ZAP”

- we can download zap our pc by following link.
  Link - zaproxy.org/download/
  It supports many operating systems, and we can choose the relevant setup



Download ZAP

Checksums for all of the ZAP downloads are maintained on the 2.9.0 Release Page and in the relevant version files.

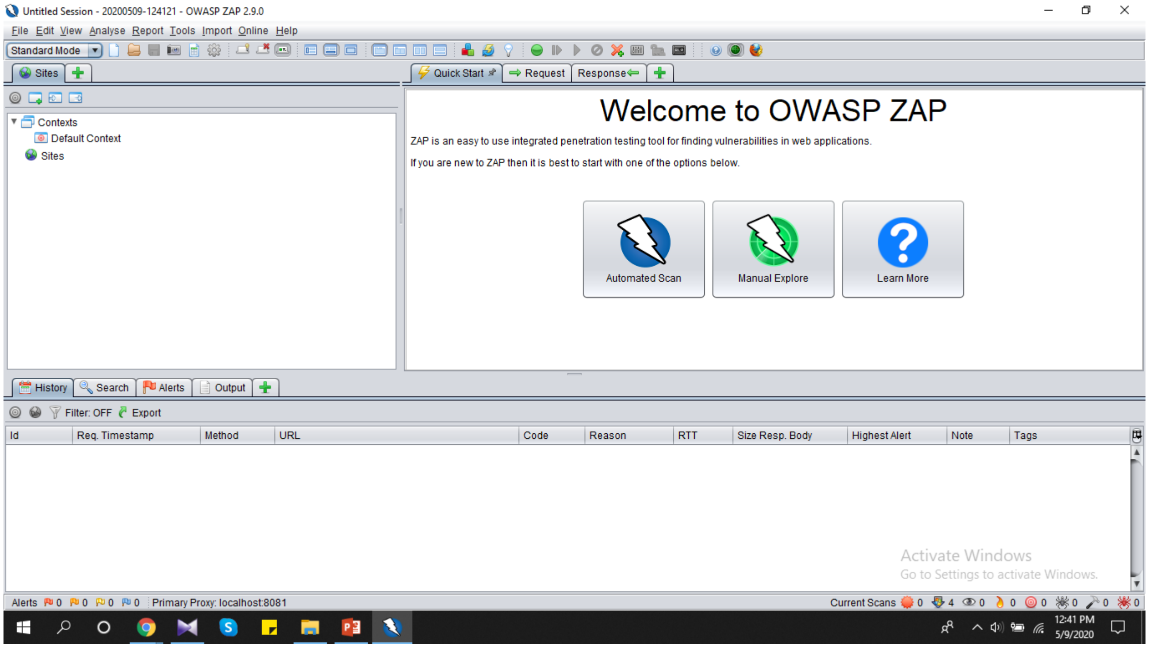
As with all software we strongly recommend that ZAP is only installed and used on operating systems and JREs that are fully patched and actively maintained.

ZAP 2.9.0

Windows (64) Installer	94 MB	Download
Windows (32) Installer	94 MB	Download
Linux Installer	94 MB	Download
Linux Package	92 MB	Download

Fig 4.1: downloading ZAP

- After installing zap setup open it. this is the zap user interface.



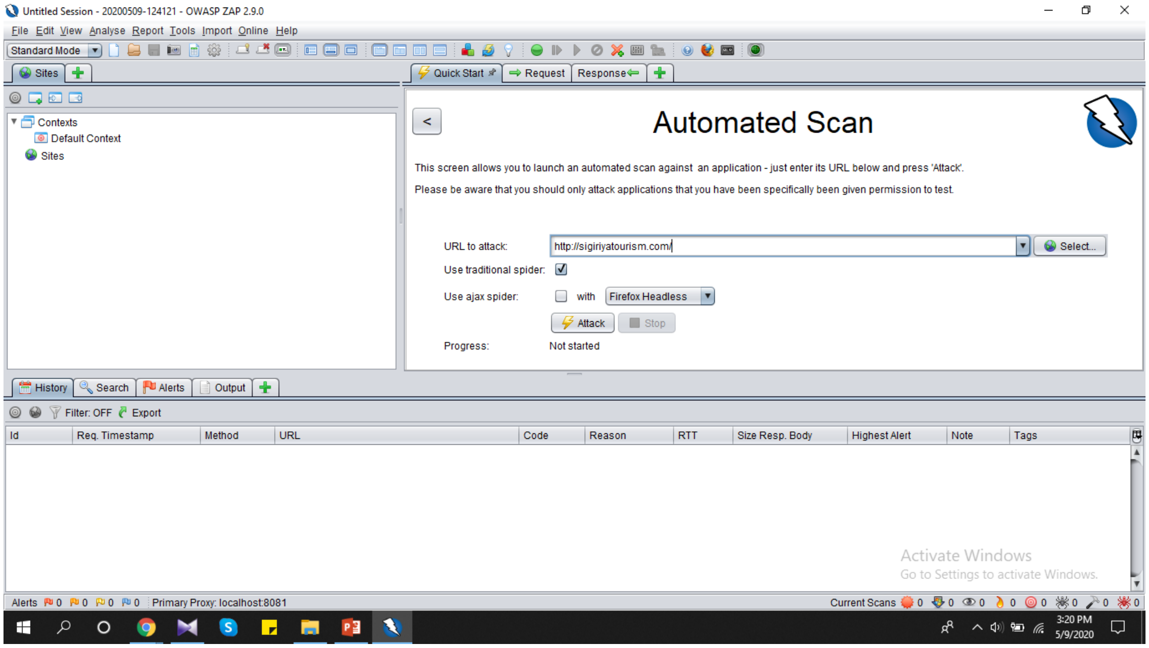
Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Fig 4.2 : ZAP User interface

- It has two primary scan type as automated and manual. Choose the manual scan type because we can get more details about web application on this scan type.



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://sigiriyatourism.com/

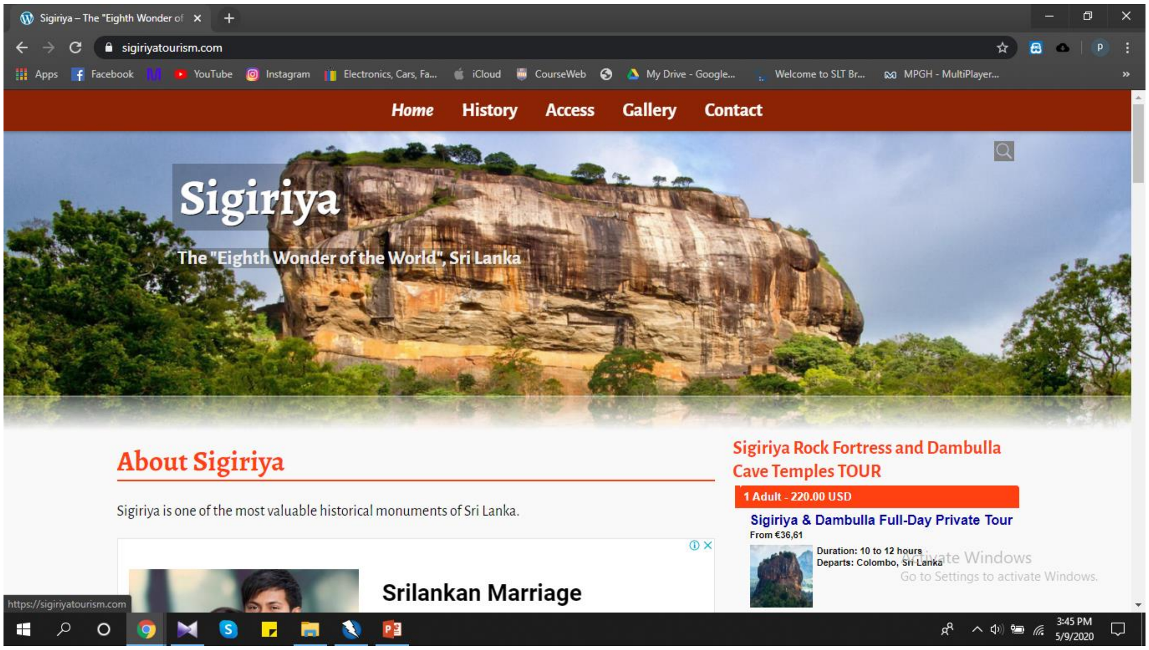
Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Not started

Fig 4.3 : choose scan type

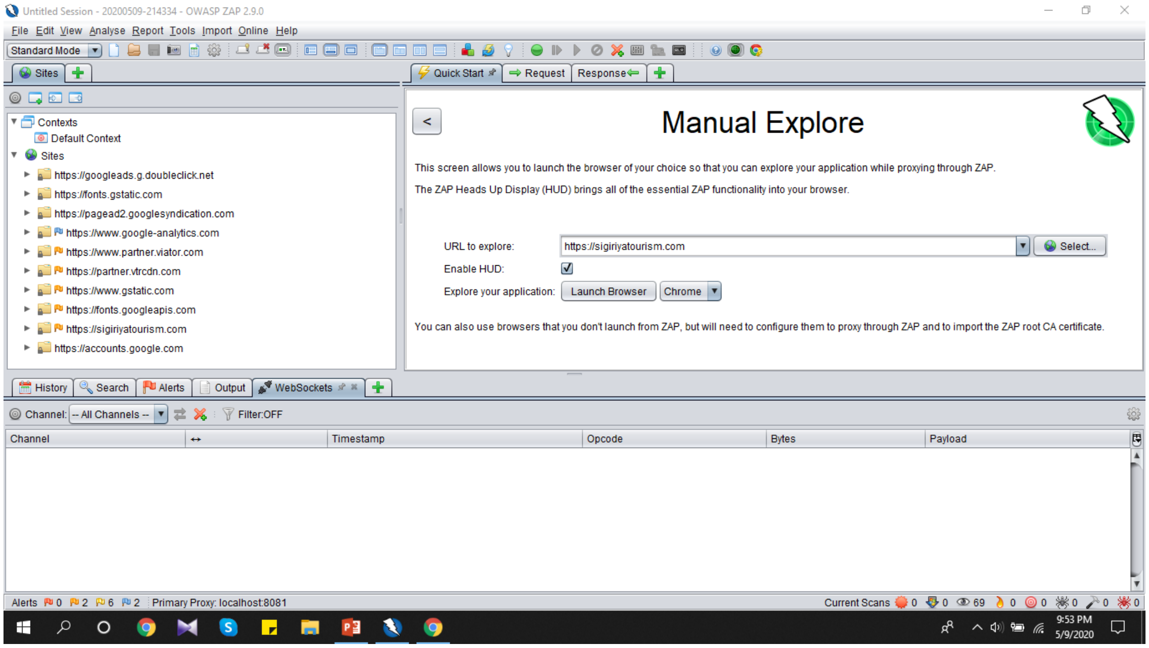
- Get a relevant web sites link. I choose sigiriyatourisum.com as websites for audit. It is SriLankan websites and includes much information about Sigiriya and tourism hotel about the Sigiriya area.



Sigiriya is one of the most valuable historical monuments of Sri Lanka.

Fig 4.4 : our website

- Go to zap the user interface and choose a manual scan mood. Next, copy our website URL and copy it into the zap. Next, we can choose a web browser like Chrome or firefox. I select Chrome and click the launch browser.


Untitled Session - 20200509-214334 - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
History
Search
Alerts
Output
WebSockets
9:53 PM
5/9/2020

- Contexts
  - Default Context
- Sites
  - https://googleads.g.doubleclick.net
  - https://fonts.gstatic.com
  - https://pagead2.googlesyndication.com
  - https://www.google-analytics.com
  - https://www.partner.viator.com
  - https://partner.vtrcdn.com
  - https://www.gstatic.com
  - https://fonts.googleapis.com
  - https://sigiriyatourism.com
  - https://accounts.google.com

Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: https://sigiriyatourism.com [Select...]

Enable HUD: ☑

Explore your application: [Launch Browser] [Chrome]

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

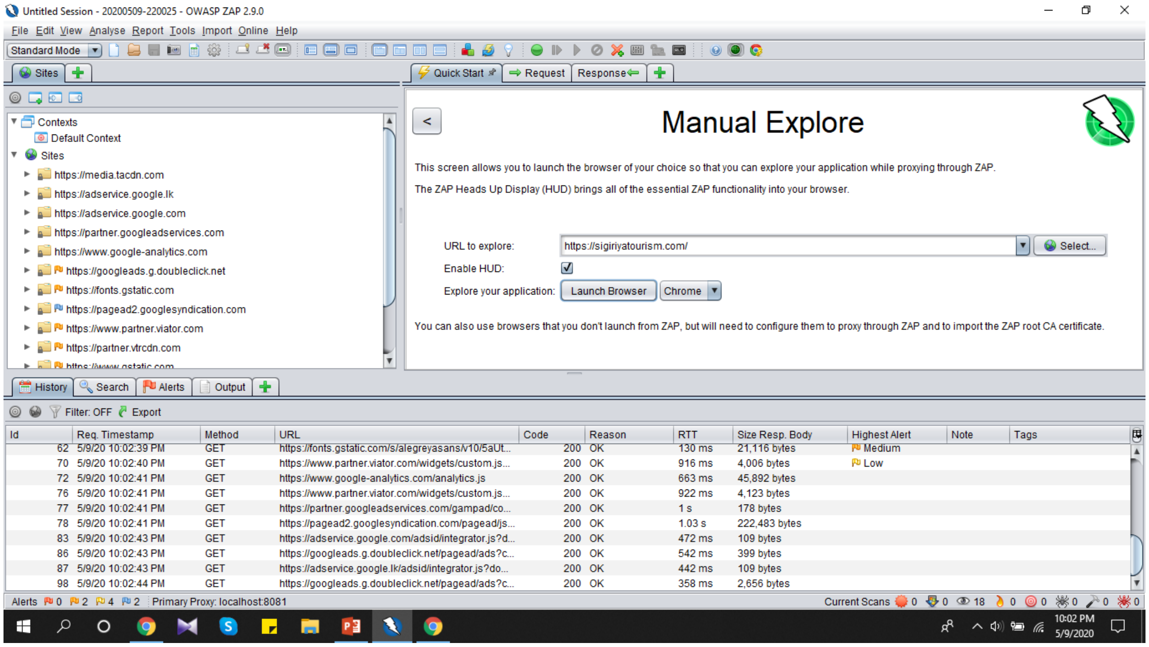
Channel: -- All Channels -- Filter:OFF

Channel	↔	Timestamp	Opcode	Bytes	Payload

Alerts 0 2 6 2 Primary Proxy: localhost:8081 Current Scans 0 0 69 0 0 0 0 0

Fig 4.5 : start scan

- Now we can see scan website the left side shows our website's backlink web site in the zap user interface


Untitled Session - 20200509-220025 - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
History
Search
Alerts
Output
Filter: OFF
Export
10:02 PM
5/9/2020

- Contexts
  - Default Context
- Sites
  - https://media.tacdn.com
  - https://adservice.google.lk
  - https://adservice.google.com
  - https://partner.googleadservices.com
  - https://www.google-analytics.com
  - https://googleads.g.doubleclick.net
  - https://fonts.gstatic.com
  - https://pagead2.googlesyndication.com
  - https://www.partner.viator.com
  - https://partner.vtrcdn.com
  - https://www.gstatic.com

Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: https://sigiriyatourism.com/ [Select...]

Enable HUD: ☑

Explore your application: [Launch Browser] [Chrome]

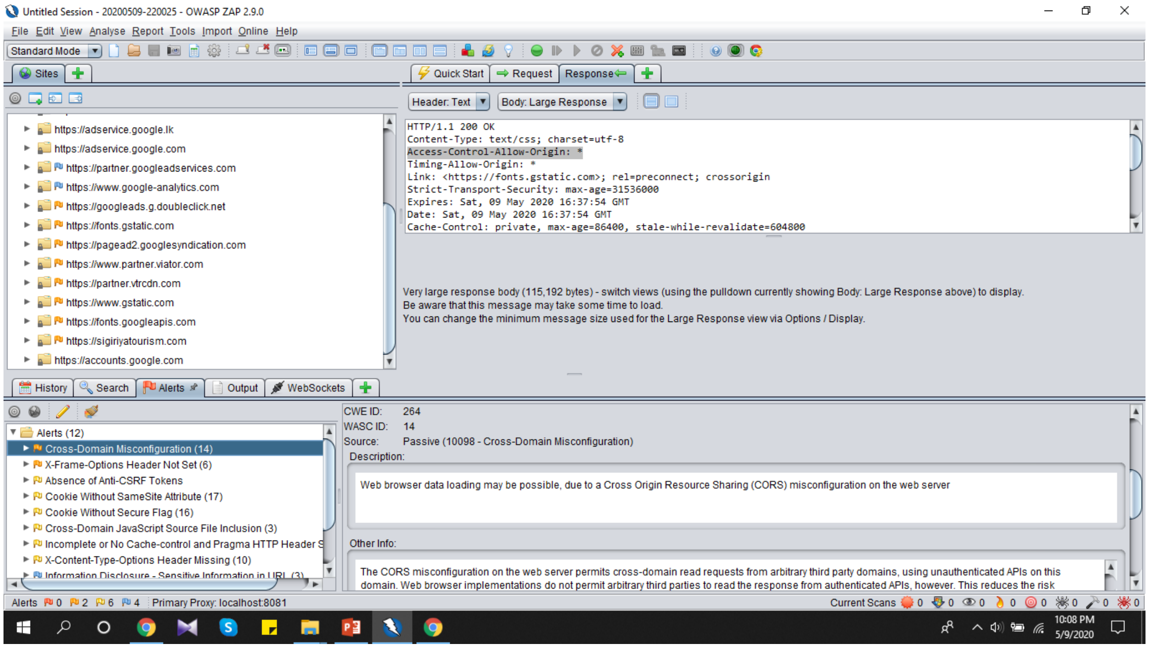
You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
62	5/9/20 10:02:39 PM	GET	https://fonts.gstatic.com/s/alegreyasans/v10/5aUt...	200	OK	130 ms	21,116 bytes	Medium		
70	5/9/20 10:02:40 PM	GET	https://www.partner.viator.com/widgets/custom.js...	200	OK	916 ms	4,006 bytes	Low		
72	5/9/20 10:02:41 PM	GET	https://www.google-analytics.com/analytics.js	200	OK	663 ms	45,892 bytes			
76	5/9/20 10:02:41 PM	GET	https://www.partner.viator.com/widgets/custom.js...	200	OK	922 ms	4,123 bytes			
77	5/9/20 10:02:41 PM	GET	https://partner.googleadservices.com/gampad/co...	200	OK	1 s	178 bytes			
78	5/9/20 10:02:41 PM	GET	https://pagead2.googlesyndication.com/pagead/js...	200	OK	1.03 s	222,483 bytes			
83	5/9/20 10:02:43 PM	GET	https://adservice.google.com/adsid/integrator.js?d...	200	OK	472 ms	109 bytes			
86	5/9/20 10:02:43 PM	GET	https://googleads.g.doubleclick.net/pagead/ads?c...	200	OK	542 ms	399 bytes			
87	5/9/20 10:02:43 PM	GET	https://adservice.google.lk/adsid/integrator.js?do...	200	OK	442 ms	109 bytes			
98	5/9/20 10:02:44 PM	GET	https://googleads.g.doubleclick.net/pagead/ads?c...	200	OK	358 ms	2,656 bytes			

Alerts 0 2 4 2 Primary Proxy: localhost:8081 Current Scans 0 0 18 0 0 0 0 0

Fig 4.6 : scaning

- After the scan, we can look like this interface, and it has a backlink site and alert information. Mention more details about the alert. Alert display 4 colors like red orange yellow blue. This color shows the risk level of alert.



- https://adservice.google.lk
- https://adservice.google.com
- https://partner.googleadservices.com
- https://www.google-analytics.com
- https://googleads.g.doubleclick.net
- https://fonts.gstatic.com
- https://pagead2.googlesyndication.com
- https://www.partner.viator.com
- https://partner.vtrcdn.com
- https://www.gstatic.com
- https://fonts.googleapis.com
- https://sigiriyatourism.com
- https://accounts.google.com

```
HTTP/1.1 200 OK
Content-Type: text/css; charset=utf-8
Access-Control-Allow-Origin: *
Timing-Allow-Origin: *
Link: <https://fonts.gstatic.com>; rel=preconnect; crossorigin
Strict-Transport-Security: max-age=31536000
Expires: Sat, 09 May 2020 16:37:54 GMT
Date: Sat, 09 May 2020 16:37:54 GMT
Cache-Control: private, max-age=86400, stale-while-revalidate=604800
```

Very large response body (115,192 bytes) - switch views (using the pulldown currently showing Body: Large Response above) to display.
Be aware that this message may take some time to load.
You can change the minimum message size used for the Large Response view via Options / Display.

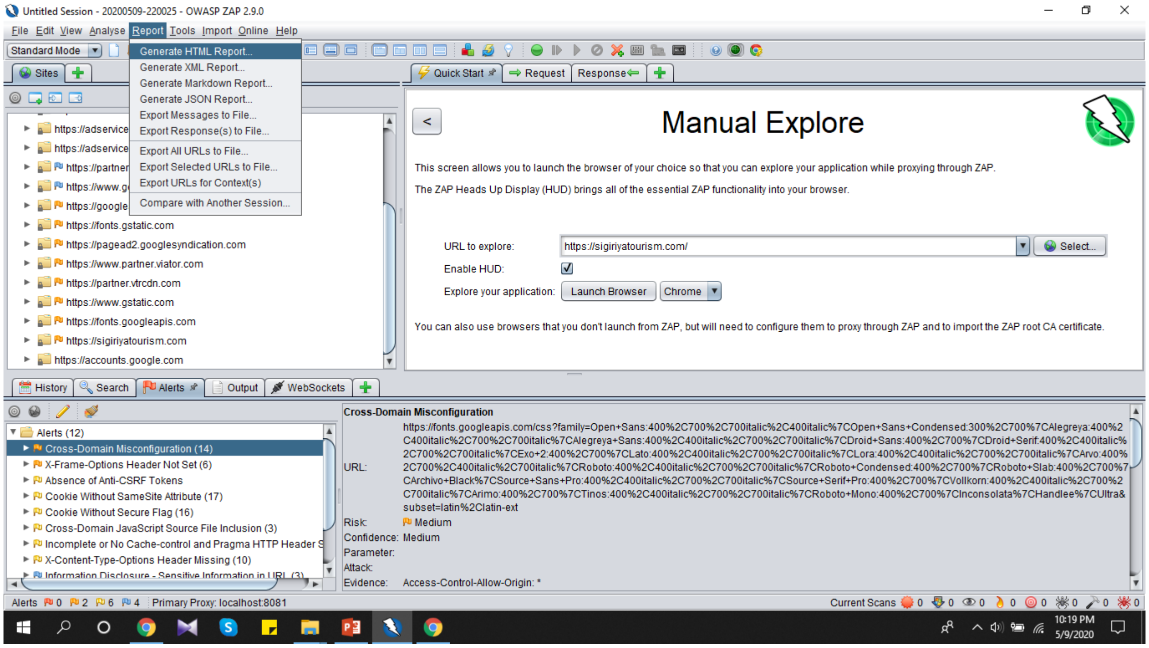
Alerts (12)
- Cross-Domain Misconfiguration (14)
- X-Frame-Options Header Not Set (6)
- Absence of Anti-CSRF Tokens
- Cookie Without SameSite Attribute (17)
- Cookie Without Secure Flag (16)
- Cross-Domain JavaScript Source File Inclusion (3)
- Incomplete or No Cache-control and Pragma HTTP Header S
- X-Content-Type-Options Header Missing (10)
- Information Disclosure - Sensitive Information in URL (3)

CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Description:
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
Other Info:
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk

Alerts 🏴 0 🏴 2 🏴 6 🏴 4 Primary Proxy: localhost:8081
Current Scans 0 0 0 0 0 0 0 0

Fig 4.7 : after scan website

- We can get an audit report go to report and select a need report format. I select HTML report


Untitled Session - 20200509-220025 - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Generate HTML Report...
Generate XML Report...
Generate Markdown Report...
Generate JSON Report...
Export Messages to File...
Export Response(s) to File...
Export All URLs to File...
Export Selected URLs to File...
Export URLs for Context(s)
Compare with Another Session...
Sites
Quick Start
Request
Response
History
Search
Alerts
Output
WebSockets
Select...
Current Scans 0 0 0 0 0 0 0 0
10:19 PM
5/9/2020

https://adservice
https://adservice
https://partner
https://www.g
https://google
https://fonts.gstatic.com
https://pagead2.googlesyndication.com
https://www.partner.viator.com
https://partner.vtrcdn.com
https://www.gstatic.com
https://fonts.googleapis.com
https://sigiriyatourism.com
https://accounts.google.com

Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: https://sigiriyatourism.com/
Enable HUD: ☑
Explore your application: Launch Browser Chrome

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

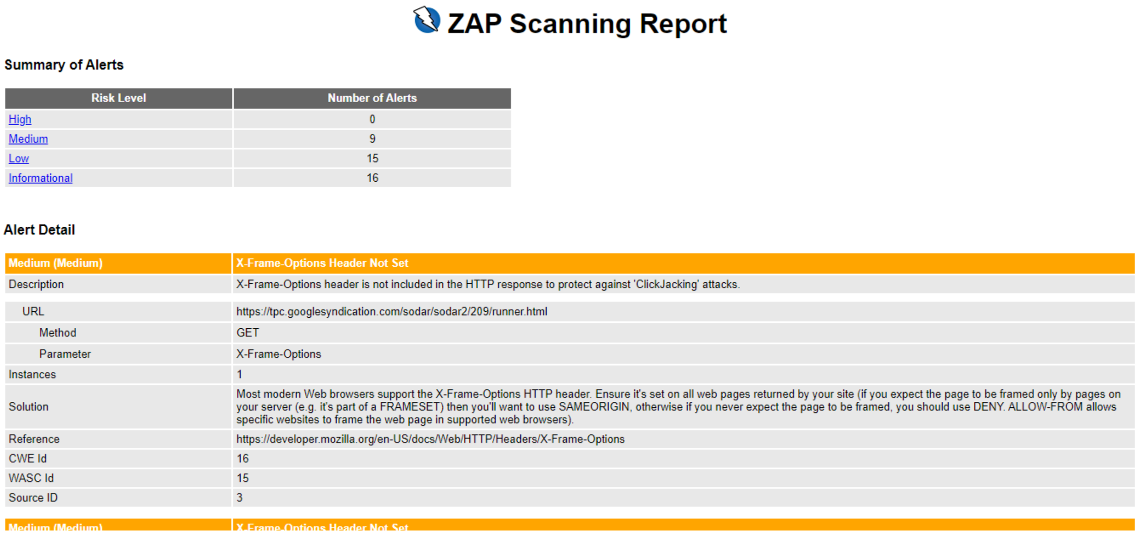
Alerts (12)
- Cross-Domain Misconfiguration (14)
- X-Frame-Options Header Not Set (6)
- Absence of Anti-CSRF Tokens
- Cookie Without SameSite Attribute (17)
- Cookie Without Secure Flag (16)
- Cross-Domain JavaScript Source File Inclusion (3)
- Incomplete or No Cache-control and Pragma HTTP Header S
- X-Content-Type-Options Header Missing (10)
- Information Disclosure - Sensitive Information in URL (3)

Cross-Domain Misconfiguration
URL: https://fonts.googleapis.com/css?family=Open+Sans:400%2C700%2C700italic%2C400italic%7COpen+Sans+Condensed:300%2C700%7CAlegreya:400%2C400italic%2C700%2C700italic%7CAlegreya+Sans:400%2C400italic%2C700%2C700italic%7CDroid+Sans:400%2C700%7CDroid+Serif:400%2C400italic%2C700%2C700italic%7CExo+2:400%2C700%7CLato:400%2C400italic%2C700%2C700italic%7CLora:400%2C400italic%2C700%2C700italic%7CArvo:400%2C700%2C400italic%2C700italic%7CRoboto:400%2C400italic%2C700%2C700italic%7CRoboto+Condensed:400%2C700%7CRoboto+Slab:400%2C700%7CArchivo+Black%7CSource+Sans+Pro:400%2C400italic%2C700%2C700italic%7CSource+Serif+Pro:400%2C700%7CVollkorn:400%2C400italic%2C700%2C700italic%7CArimo:400%2C700%7CTinos:400%2C400italic%2C700%2C700italic%7CRoboto+Mono:400%2C700%7CInconsolata%7CHandlee%7CUltra&subset=latin%2Clatin-ext
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *

Alerts 0 2 6 4 Primary Proxy: localhost:8081

Fig 4.8 : generate report

- After a few seconds, generate a scan report and its open web browser. Firstly scan report has a summary of alerts. Its have a risk level and how much of alert in the web site. Include alert details, as one by one. We can show more information about this alert in the sections. Zap tools show 40 alerts and give a solution in scan repot for every alert. No high-risk level attacks for the Sigiriya tourism web site. High-risk level attacks show a red color. Show medium risk level alert as orange color and yellow color show low-risk level alert. Blue color shows information alerts.



ZAP Scanning Report

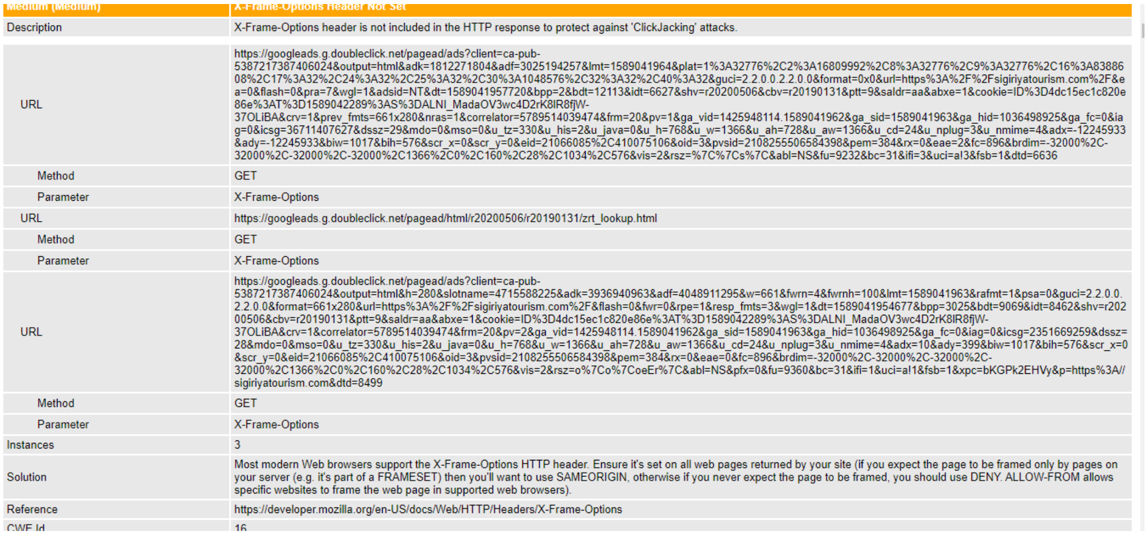
Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	9
Low	15
Informational	16

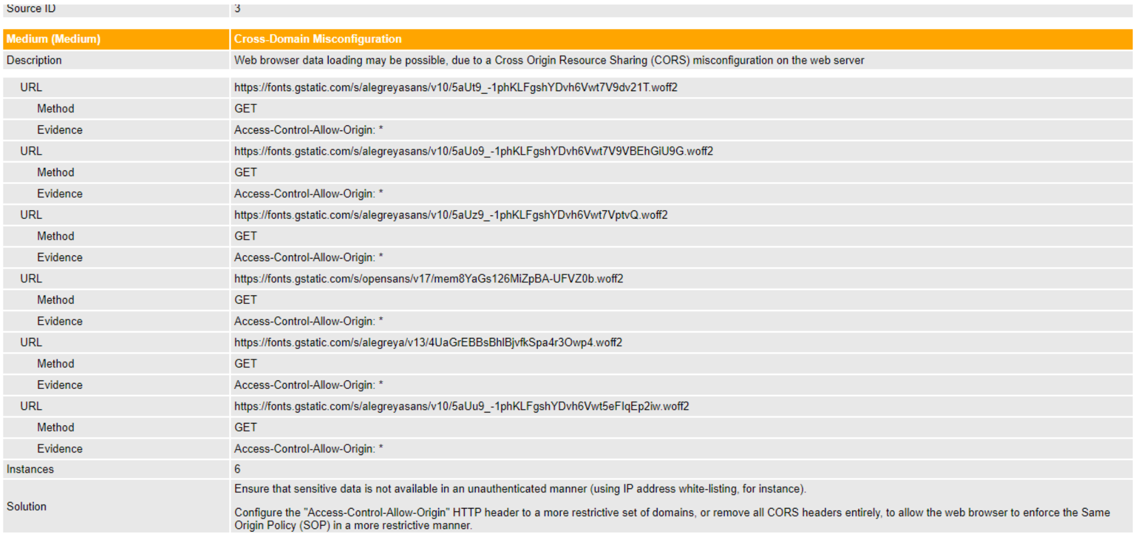
Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://tpc.googlesyndication.com/sodar/sodar2/209/runner.html
Method	GET
Parameter	X-Frame-Options
Instances	1
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	16
WASC Id	15
Source ID	3

Medium (Medium)	X-Frame-Options Header Not Set

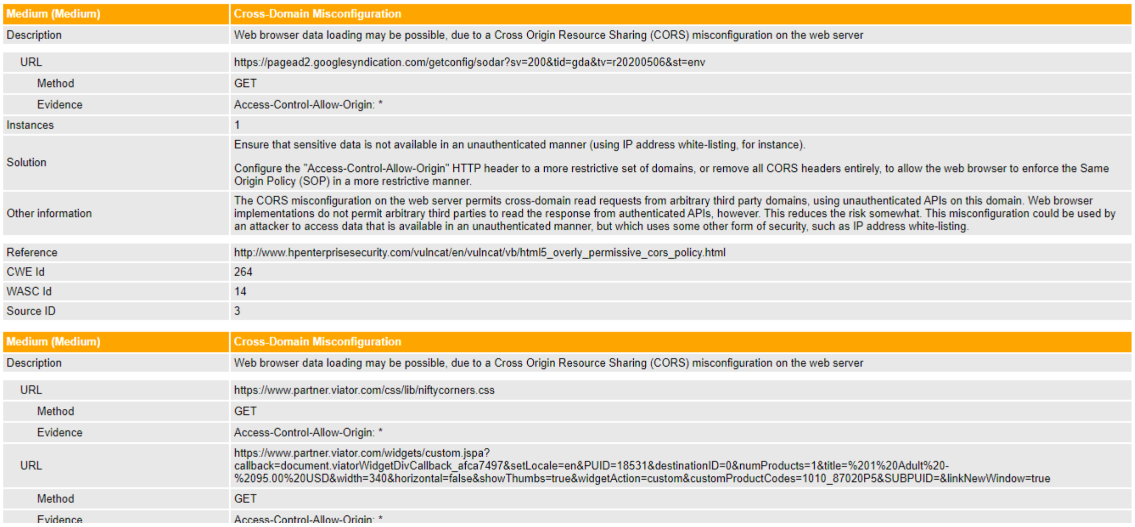


Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&adk=1812271804&adf=3025194257&lmt=1589041964&plat=1%3A32776%2C2%3A16809992%2C8%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32%2C40%3A32&guci=2.2.0.0.2.2.0.0&format=0x0&url=https%3A%2F%2Fsigiriyatourism.com%2F&ea=0&flash=0&pra=7&wgl=1&adsid=NT&dt=1589041957720&bpp=2&bdt=12113&idt=6627&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c820e86e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8IR8fjW-37OLiBA&crv=1&prev_fmts=661x280&nras=1&correlator=5789514039474&frm=20&pv=1&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=36711407627&dssz=29&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=-12245933&ady=-12245933&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=2&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=%7C%7Cs%7C&abl=NS&fu=9232&bc=31&ifi=3&uci=a!3&fsb=1&dtd=6636
Method	GET
Parameter	X-Frame-Options
URL	https://googleads.g.doubleclick.net/pagead/html/r20200506/r20190131/zrt_lookup.html
Method	GET
Parameter	X-Frame-Options
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&h=280&slotname=4715588225&adk=3936940963&adf=4048911295&w=661&fwrn=4&fwrnh=100&lmt=1589041963&rafmt=1&psa=0&guci=2.2.0.0.2.2.0.0&format=661x280&url=https%3A%2F%2Fsigiriyatourism.com%2F&flash=0&fwr=0&rpe=1&resp_fmts=3&wgl=1&dt=1589041954677&bpp=3025&bdt=9069&idt=8462&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c820e86e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8IR8fjW-37OLiBA&crv=1&correlator=5789514039474&frm=20&pv=2&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=2351669259&dssz=28&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=10&ady=399&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=0&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=o%7Co%7CoeEr%7C&abl=NS&pfx=0&fu=9360&bc=31&ifi=1&uci=a!1&fsb=1&xpc=bKGPk2EHVy&p=https%3A//sigiriyatourism.com&dtd=8499
Method	GET
Parameter	X-Frame-Options
Instances	3
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	16



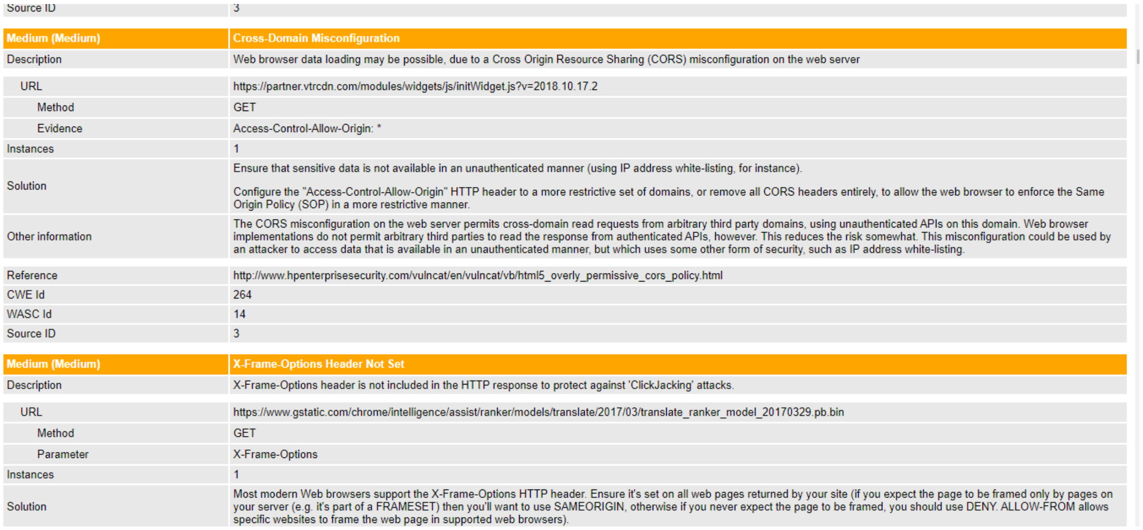
Source ID	3

Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://fonts.gstatic.com/s/alegreyasans/v10/5aUt9_-1phKLFgshYDvh6Vwt7V9dv21T.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://fonts.gstatic.com/s/alegreyasans/v10/5aUo9_-1phKLFgshYDvh6Vwt7V9VBEhGiU9G.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://fonts.gstatic.com/s/alegreyasans/v10/5aUz9_-1phKLFgshYDvh6Vwt7VptvQ.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://fonts.gstatic.com/s/opensans/v17/mem8YaGs126MiZpBA-UFVZ0b.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://fonts.gstatic.com/s/alegreya/v13/4UaGrEBBsBhlBjvfkSpa4r3Owp4.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://fonts.gstatic.com/s/alegreyasans/v10/5aUu9_-1phKLFgshYDvh6Vwt5eFIqEp2iw.woff2
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	6
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.



Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://pagead2.googlesyndication.com/getconfig/sodar?sv=200&tid=gda&tv=r20200506&st=env
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html
CWE Id	264
WASC Id	14
Source ID	3

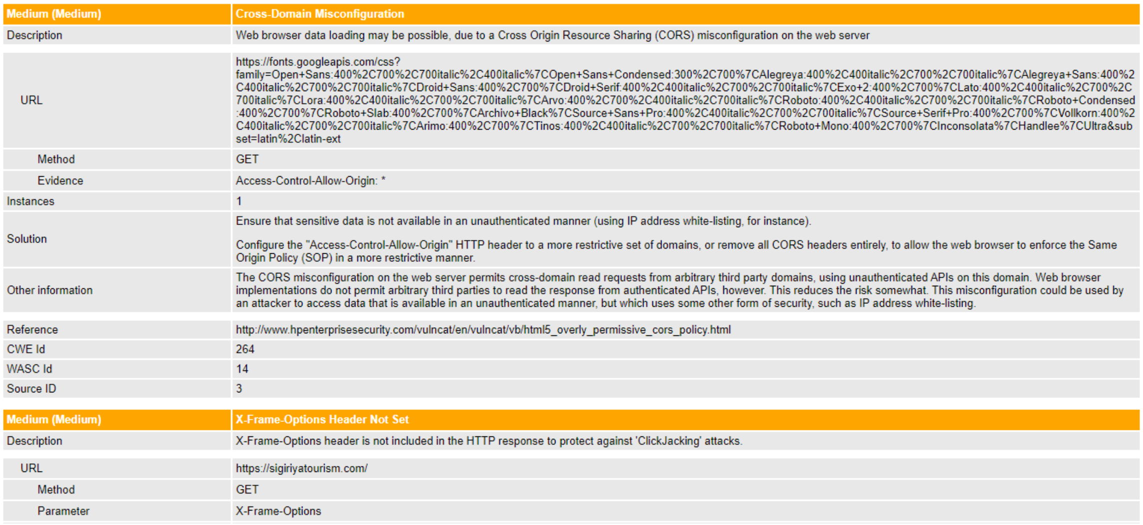
Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://www.partner.viator.com/css/lib/niftycorners.css
Method	GET
Evidence	Access-Control-Allow-Origin: *
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Method	GET
Evidence	Access-Control-Allow-Origin: *



Source ID	3

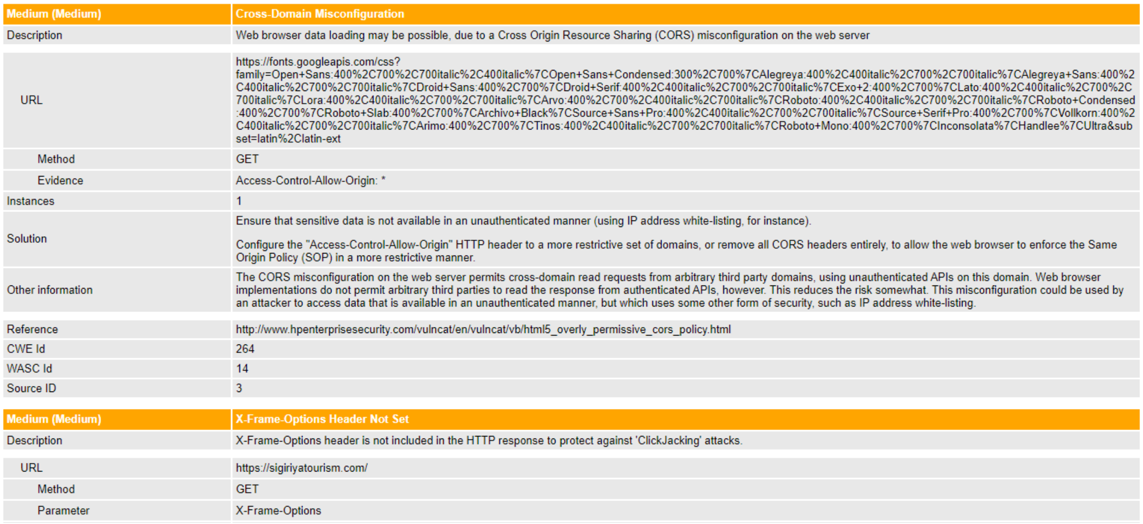
Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://partner.vtrcdn.com/modules/widgets/js/initWidget.js?v=2018.10.17.2
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html
CWE Id	264
WASC Id	14
Source ID	3

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://www.gstatic.com/chrome/intelligence/assist/ranker/models/translate/2017/03/translate_ranker_model_20170329.pb.bin
Method	GET
Parameter	X-Frame-Options
Instances	1
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).



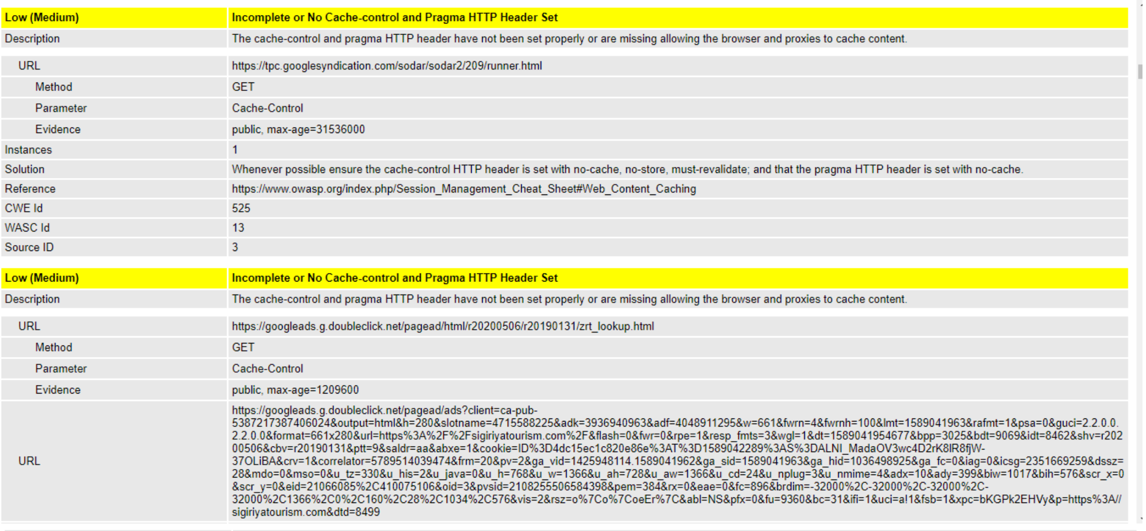
Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://fonts.googleapis.com/css?family=Open+Sans:400%2C700%2C700italic%2C400italic%7COpen+Sans+Condensed:300%2C700%7CAlegreya:400%2C400italic%2C700%2C700italic%7CAlegreya+Sans:400%2C400italic%2C700%2C700italic%7CDroid+Sans:400%2C700%7CDroid+Serif:400%2C400italic%2C700%2C700italic%7CExo+2:400%2C700%7CLato:400%2C400italic%2C700%2C700italic%7CLora:400%2C400italic%2C700%2C700italic%7CArvo:400%2C700%2C400italic%2C700italic%7CRoboto:400%2C400italic%2C700%2C700italic%7CRoboto+Condensed:400%2C700%7CRoboto+Slab:400%2C700%7CArchivo+Black%7CSource+Sans+Pro:400%2C400italic%2C700%2C700italic%7CSource+Serif+Pro:400%2C700%7CVollkorn:400%2C400italic%2C700%2C700italic%7CArimo:400%2C700%7CTinos:400%2C400italic%2C700%2C700italic%7CRoboto+Mono:400%2C700%7CInconsolata%7CHandlee%7CUltra&subset=latin%2Clatin-ext
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html
CWE Id	264
WASC Id	14
Source ID	3

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://sigiriyatourism.com/
Method	GET
Parameter	X-Frame-Options



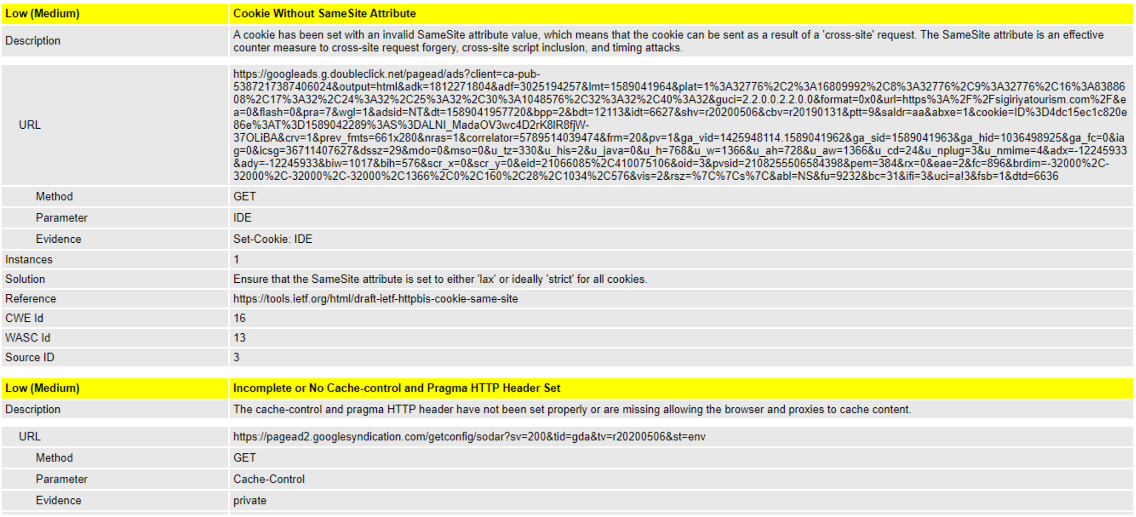
Medium (Medium)	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://fonts.googleapis.com/css?family=Open+Sans:400%2C700%2C700italic%2C400italic%7COpen+Sans+Condensed:300%2C700%7CAlegreya:400%2C400italic%2C700%2C700italic%7CAlegreya+Sans:400%2C400italic%2C700%2C700italic%7CDroid+Sans:400%2C700%7CDroid+Serif:400%2C400italic%2C700%2C700italic%7CExo+2:400%2C700%7CLato:400%2C400italic%2C700%2C700italic%7CLora:400%2C400italic%2C700%2C700italic%7CArvo:400%2C700%2C400italic%2C700italic%7CRoboto:400%2C400italic%2C700%2C700italic%7CRoboto+Condensed:400%2C700%7CRoboto+Slab:400%2C700%7CArchivo+Black%7CSource+Sans+Pro:400%2C400italic%2C700%2C700italic%7CSource+Serif+Pro:400%2C700%7CVollkorn:400%2C400italic%2C700%2C700italic%7CArimo:400%2C700%7CTinos:400%2C400italic%2C700%2C700italic%7CRoboto+Mono:400%2C700%7CInconsolata%7CHandlee%7CUltra&subset=latin%2Clatin-ext
Method	GET
Evidence	Access-Control-Allow-Origin: *
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Other information	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Reference	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/vb/html5_overly_permissive_cors_policy.html
CWE Id	264
WASC Id	14
Source ID	3

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://sigiriyatourism.com/
Method	GET
Parameter	X-Frame-Options



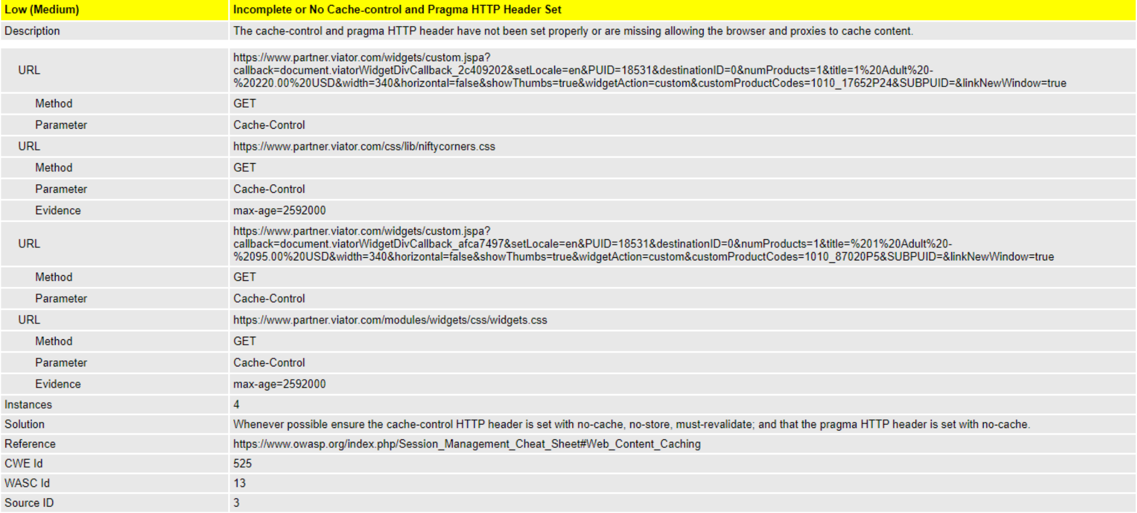
Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://tpc.googlesyndication.com/sodar/sodar2/209/runner.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=31536000
Instances	1
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3

Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://googleads.g.doubleclick.net/pagead/html/r20200506/r20190131/zrt_lookup.html
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=1209600
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&h=280&slotname=4715588225&adk=3936940963&adf=4048911295&w=661&fwrn=4&fwrnh=100&lmt=1589041963&rafmt=1&psa=0&guci=2.2.0.0.2.2.0.0&format=661x280&url=https%3A%2F%2Fsigiriyatourism.com%2F&flash=0&fwr=0&rpe=1&resp_fmts=3&wgl=1&dt=1589041954677&bpp=3025&bdt=9069&idt=8462&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c820e86e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8lR8fjW-37OLiBA&crv=1&correlator=5789514039474&frm=20&pv=2&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=2351669259&dssz=28&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=10&ady=399&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=0&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=o%7Co%7CoeEr%7C&abl=NS&pfx=0&fu=9360&bc=31&ifi=1&uci=a!1&fsb=1&xpc=bKGPk2EHVy&p=https%3A//sigiriyatourism.com&dtd=8499

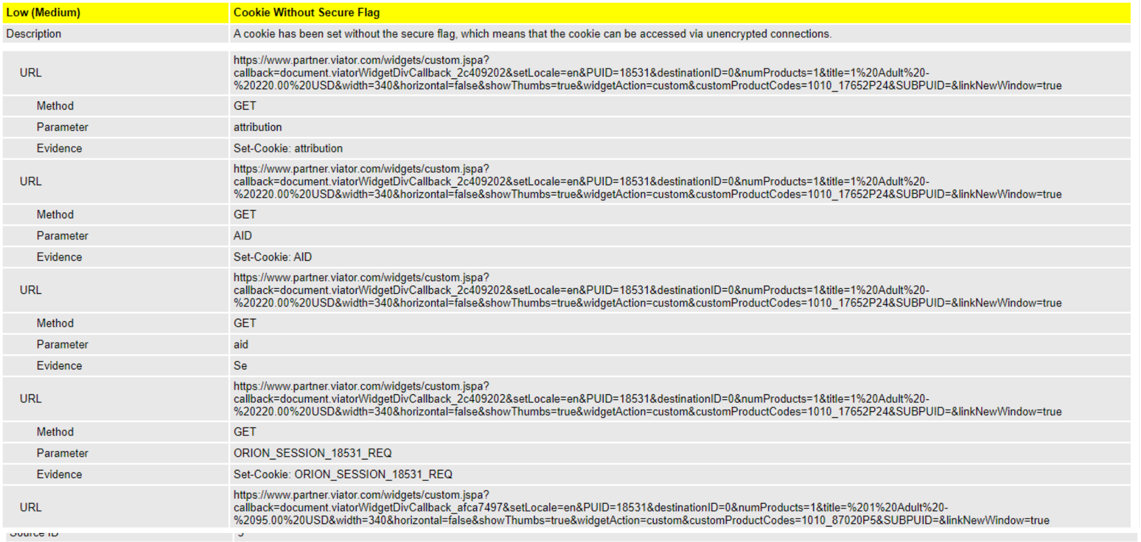


Low (Medium)	Cookie Without SameSite Attribute
Description	A cookie has been set with an invalid SameSite attribute value, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&adk=1812271804&adf=3025194257&lmt=1589041964&plat=1%3A32776%2C2%3A16809992%2C8%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32%2C40%3A32&guci=2.2.0.0.2.2.0.0&format=0x0&url=https%3A%2F%2Fsigiriyatourism.com%2F&ea=0&flash=0&pra=7&wgl=1&adsid=NT&dt=1589041957720&bpp=2&bdt=12113&idt=6627&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c820e86e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8lR8fjW-37OLiBA&crv=1&prev_fmts=661x280&nras=1&correlator=5789514039474&frm=20&pv=1&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=36711407627&dssz=29&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=-12245933&ady=-12245933&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=2&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=%7C%7Cs%7C&abl=NS&fu=9232&bc=31&ifi=3&uci=a!3&fsb=1&dtd=6636
Method	GET
Parameter	IDE
Evidence	Set-Cookie: IDE
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	16
WASC Id	13
Source ID	3

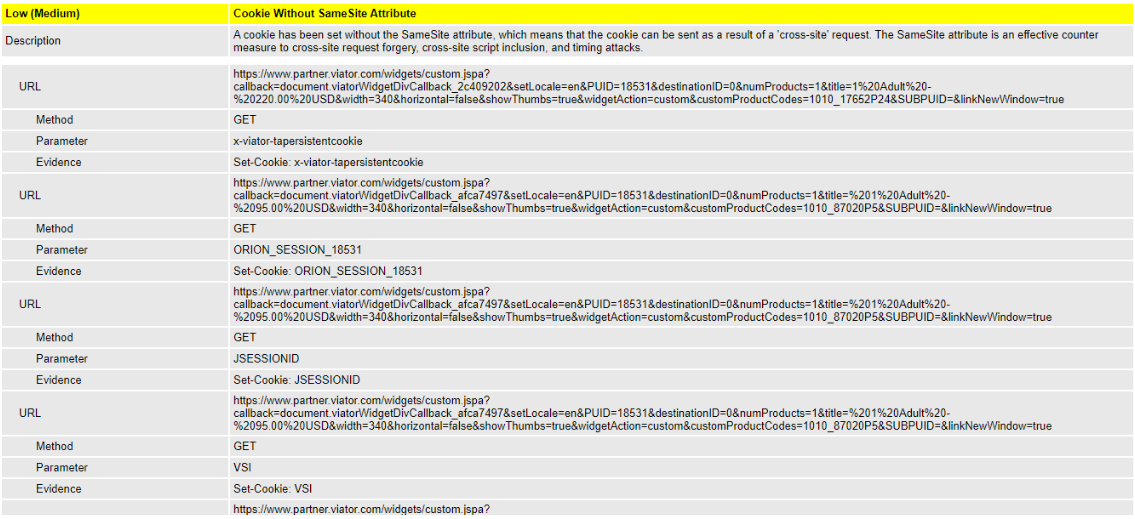
Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://pagead2.googlesyndication.com/getconfig/sodar?sv=200&tid=gda&tv=r20200506&st=env
Method	GET
Parameter	Cache-Control
Evidence	private



Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	Cache-Control
URL	https://www.partner.viator.com/css/lib/niftycorners.css
Method	GET
Parameter	Cache-Control
Evidence	max-age=2592000
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	Cache-Control
URL	https://www.partner.viator.com/modules/widgets/css/widgets.css
Method	GET
Parameter	Cache-Control
Evidence	max-age=2592000
Instances	4
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3



Low (Medium)	Cookie Without Secure Flag
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	attribution
Evidence	Set-Cookie: attribution
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	AID
Evidence	Set-Cookie: AID
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	aid
Evidence	Se
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	ORION_SESSION_18531_REQ
Evidence	Set-Cookie: ORION_SESSION_18531_REQ
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Source ID	3



Low (Medium)	Cookie Without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	x-viator-tapersistentcookie
Evidence	Set-Cookie: x-viator-tapersistentcookie
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	ORION_SESSION_18531
Evidence	Set-Cookie: ORION_SESSION_18531
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	JSESSIONID
Evidence	Set-Cookie: JSESSIONID
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	VSI
Evidence	Set-Cookie: VSI
	https://www.partner.viator.com/widgets/custom.jspa?

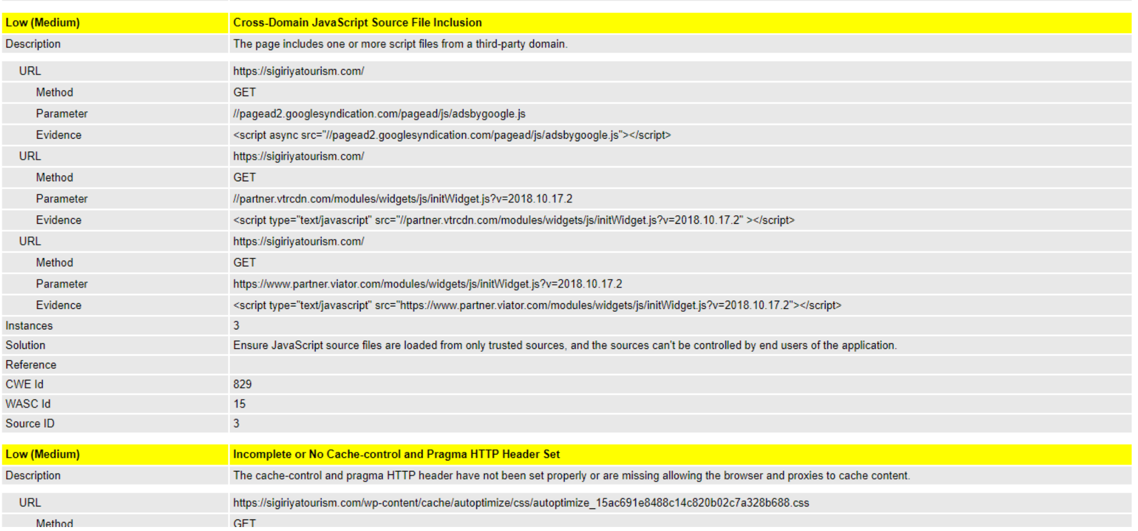
Low (Medium)	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted 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.
URL	https://www.partner.viator.com/css/lib/niftycorners.css
Method	GET
Parameter	X-Content-Type-Options
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	X-Content-Type-Options
URL	https://www.partner.viator.com/modules/widgets/js/initWidget.js?v=2018.10.17.2
Method	GET
Parameter	X-Content-Type-Options
URL	https://www.partner.viator.com/modules/widgets/css/widgets.css
Method	GET
Parameter	X-Content-Type-Options
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Parameter	X-Content-Type-Options
Instances	5
Solution	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. 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.

Low (Medium)	X-Content-Type-Options Header Missing
Description	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.
URL	https://partner.vtrcdn.com/modules/widgets/js/initWidget.js?v=2018.10.17.2
Method	GET
Parameter	X-Content-Type-Options
Instances	1
Solution	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. 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.
Other information	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scanner will not alert on client or server error responses.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://www.gstatic.com/chrome/intelligence/assist/ranker/models/translate/2017/03/translate_ranker_model_20170329.pb.bin
Method	GET
Parameter	Cache-Control
Evidence	public, max-age=31536000

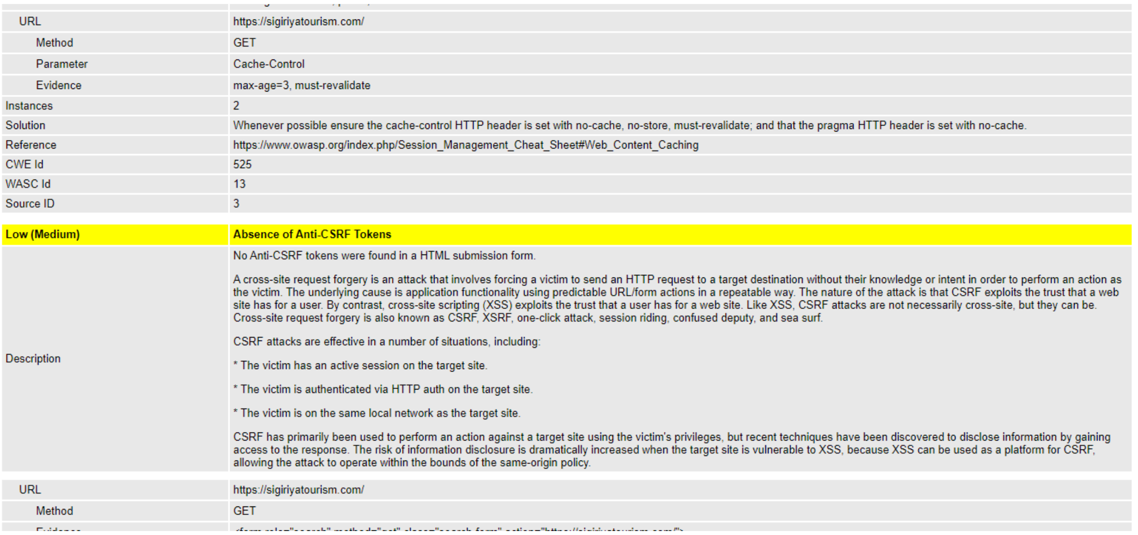
Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://fonts.googleapis.com/css?family=Open+Sans:400%2C700%2C700italic%2C400italic%7COpen+Sans+Condensed:300%2C700%7CAlegreya:400%2C400italic%2C700%2C700italic%7CAlegreya+Sans:400%2C400italic%2C700%2C700italic%7CDroid+Sans:400%2C700%7CDroid+Serif:400%2C400italic%2C700%2C700italic%7CExo+2:400%2C700%7CLato:400%2C400italic%2C700%2C700italic%7CLora:400%2C400italic%2C700%2C700italic%7CArvo:400%2C700%2C400italic%2C700italic%7CRoboto:400%2C400italic%2C700%2C700italic%7CRoboto+Condensed:400%2C700%7CRoboto+Slab:400%2C700%7CArchivo+Black%7CSource+Sans+Pro:400%2C400italic%2C700%2C700italic%7CSource+Serif+Pro:400%2C700%7CVollkorn:400%2C400italic%2C700%2C700italic%7CArimo:400%2C700%7CTinos:400%2C400italic%2C700%2C700italic%7CRoboto+Mono:400%2C700%7CInconsolata%7CHandlee%7CUltra&subset=latin%2Clatin-ext
Method	GET
Parameter	Cache-Control
Evidence	private, max-age=86400, stale-while-revalidate=604800
Instances	1
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3

Low (Medium)	X-Content-Type-Options Header Missing
Description	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.
URL	https://sigiriyatourism.com/wp-content/cache/autoptimize/css/autoptimize_15ac691e8488c14c820b02c7a328b688.css
Method	GET
Parameter	X-Content-Type-Options
URL	https://sigiriyatourism.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp
Method	GET



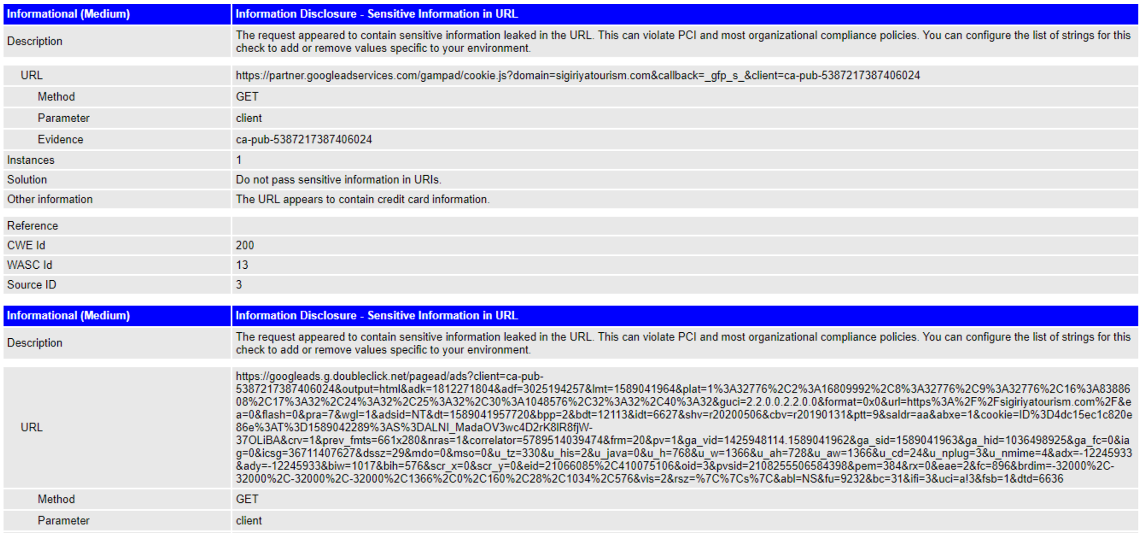
Low (Medium)	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	https://sigiriyatourism.com/
Method	GET
Parameter	//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Evidence	<script async src="//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script>
URL	https://sigiriyatourism.com/
Method	GET
Parameter	//partner.vtrcdn.com/modules/widgets/js/initWidget.js?v=2018.10.17.2
Evidence	<script type="text/javascript" src="//partner.vtrcdn.com/modules/widgets/js/initWidget.js?v=2018.10.17.2" ></script>
URL	https://sigiriyatourism.com/
Method	GET
Parameter	https://www.partner.viator.com/modules/widgets/js/initWidget.js?v=2018.10.17.2
Evidence	<script type="text/javascript" src="https://www.partner.viator.com/modules/widgets/js/initWidget.js?v=2018.10.17.2"></script>
Instances	3
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Source ID	3

Low (Medium)	Incomplete or No Cache-control and Pragma HTTP Header Set
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://sigiriyatourism.com/wp-content/cache/autoptimize/css/autoptimize_15ac691e8488c14c820b02c7a328b688.css
Method	GET



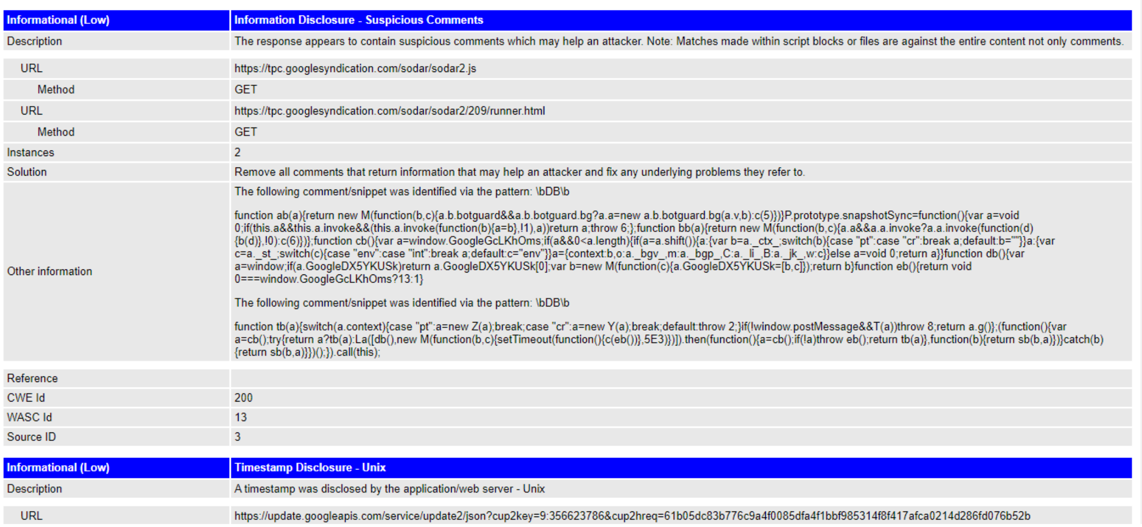
URL	https://sigiriyatourism.com/
Method	GET
Parameter	Cache-Control
Evidence	max-age=3, must-revalidate
Instances	2
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3

Low (Medium)	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://sigiriyatourism.com/
Method	GET
Evidence	<form role="search" method="get" class="search-form" action="https://sigiriyatourism.com/">



Informational (Medium)	Information Disclosure - Sensitive Information in URL
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://partner.googleadservices.com/gampad/cookie.js?domain=sigiriyatourism.com&callback=_gfp_s_&client=ca-pub-5387217387406024
Method	GET
Parameter	client
Evidence	ca-pub-5387217387406024
Instances	1
Solution	Do not pass sensitive information in URIs.
Other information	The URL appears to contain credit card information.
Reference	
CWE Id	200
WASC Id	13
Source ID	3

Informational (Medium)	Information Disclosure - Sensitive Information in URL
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&adk=1812271804&adf=3025194257&lmt=1589041964&plat=1%3A32776%2C2%3A16809992%2C8%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32%2C40%3A32&guci=2.2.0.0.2.2.0.0&format=0x0&url=https%3A%2F%2Fsigiriyatourism.com%2F&ea=0&flash=0&pra=7&wgl=1&adsid=NT&dt=1589041957720&bpp=2&bdt=12113&idt=6627&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c82086e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8lR8fjW-37OLiBA&crv=1&prev_fmts=661x280&nras=1&correlator=5789514039474&frm=20&pv=1&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=36711407627&dssz=29&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=-12245933&ady=-12245933&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=2&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=%7C%7Cs%7C&abl=NS&fu=9232&bc=31&ifi=3&uci=a!3&fsb=1&dtd=6636
Method	GET
Parameter	client

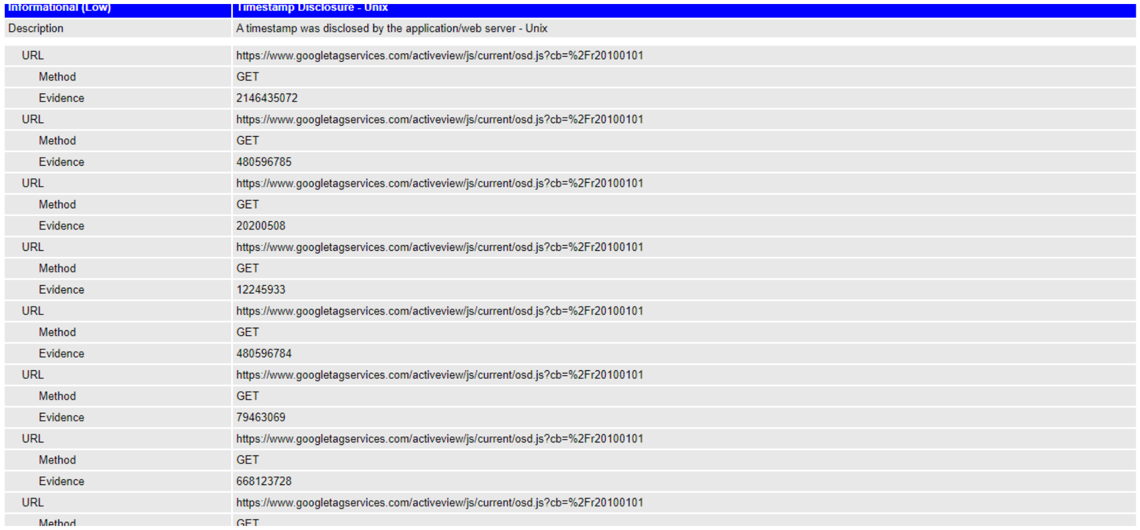


Informational (Low)	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://tpc.googlesyndication.com/sodar/sodar2.js
Method	GET
URL	https://tpc.googlesyndication.com/sodar/sodar2/209/runner.html
Method	GET
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

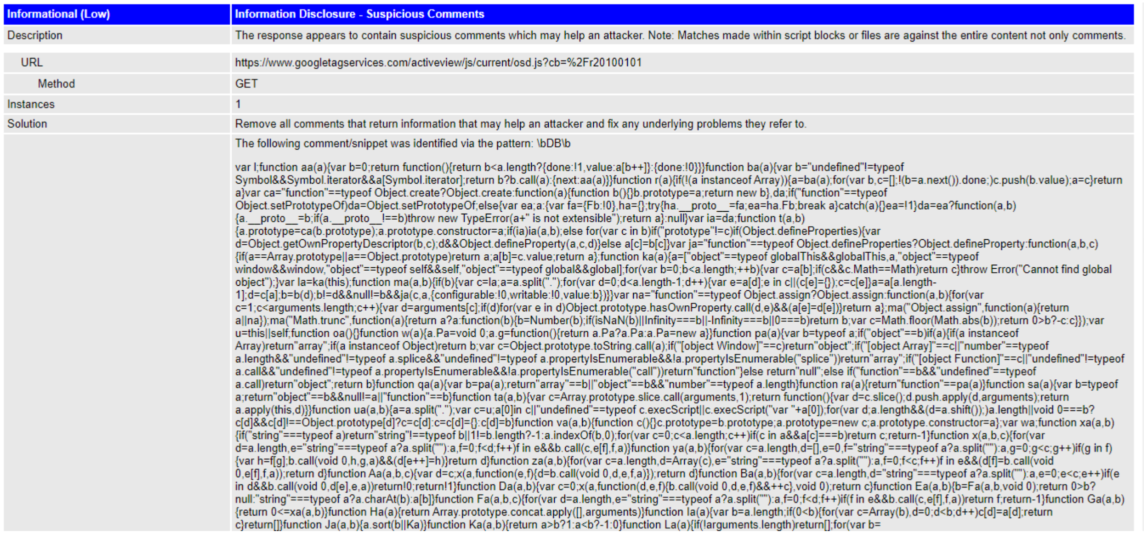
Other information	The following comment/snippet was identified via the pattern: \bDB\b
	function ab(a){return new M(function(b,c){a.b.botguard&&a.b.botguard.bg?a.a=new a.b.botguard.bg(a.v,b):c(5)})}P.prototype.snapshotSync=function(){var a=void 0;if(this.a&&this.a.invoke&&(this.a.invoke(function(b){a=b},!1),a))return a;throw 6;};function bb(a){return new M(function(b,c){a.a&&a.a.invoke?a.a.invoke(function(d){b(d)},!0):c(6)})};function cb(){var a=window.GoogleGcLKhOms;if(a&&0<a.length){if(a=a.shift()){a:{var b=a._ctx_;switch(b){case "pt":case "cr":break a;default:b=""}}a:{var c=a._st_;switch(c){case "env":case "int":break a;default:c="env"}}a={context:b,o:a._bgv_,m:a._bgp_,C:a._li_,B:a._jk_,w:c}}else a=void 0;return a}}function db(){var a=window;if(a.GoogleDX5YKUSk)return a.GoogleDX5YKUSk[0];var b=new M(function(c){a.GoogleDX5YKUSk=[b,c]});return b}function eb(){return void 0===window.GoogleGcLKhOms?13:1}
	The following comment/snippet was identified via the pattern: \bDB\b
	function tb(a){switch(a.context){case "pt":a=new Z(a);break;case "cr":a=new Y(a);break;default:throw 2;}if(!window.postMessage&&T(a))throw 8;return a.g()};(function(){var a=cb();try{return a?tb(a):La([db(),new M(function(b,c){setTimeout(function(){c(eb())},5E3)})]).then(function(){a=cb();if(!a)throw eb();return tb(a)},function(b){return sb(b,a)})}catch(b){return sb(b,a)}})();}).call(this);

Reference	
CWE Id	200
WASC Id	13
Source ID	3

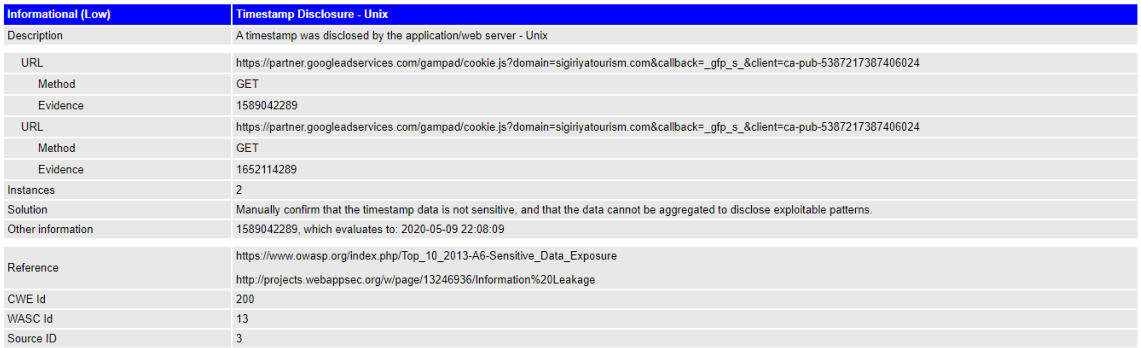
Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://update.googleapis.com/service/update2/json?cup2key=9:356623786&cup2hreq=61b05dc83b776c9a4f0085dfa4f1bbf985314f8f417afca0214d286fd076b52b



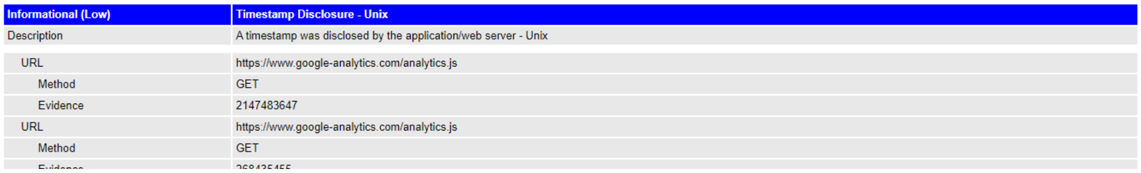
Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101
Method	GET
Evidence	2146435072
URL	https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101
Method	GET
Evidence	480596785
URL	https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101
Method	GET
Evidence	20200508
URL	https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101
Method	GET
Evidence	12245933
URL	https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101
Method	GET
Evidence	480596784
URL	https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101
Method	GET
Evidence	79463069
URL	https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101
Method	GET
Evidence	668123728
URL	https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101
Method	GET



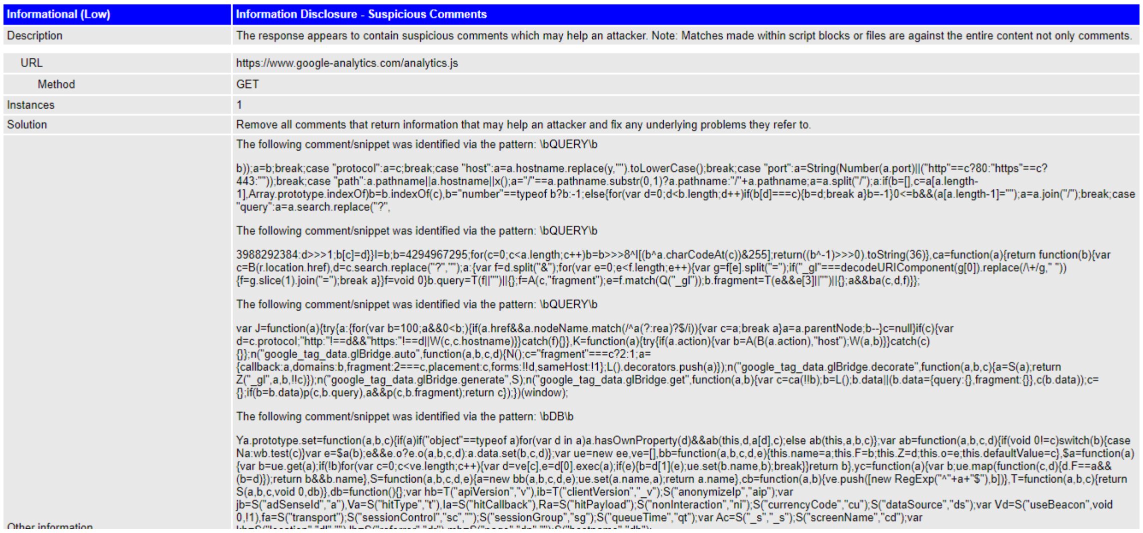
<table>
<tr><th>Informational (Low)</th><th>Information Disclosure - Suspicious Comments</th></tr>
<tr><td>Description</td><td>The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.</td></tr>
<tr><td>URL</td><td>https://www.googletagservices.com/activeview/js/current/osd.js?cb=%2Fr20100101</td></tr>
<tr><td>Method</td><td>GET</td></tr>
<tr><td>Instances</td><td>1</td></tr>
<tr><td>Solution</td><td>Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.</td></tr>
<tr><td></td><td>The following comment/snippet was identified via the pattern: \bDB\b
var l;function aa(a){var b=0;return function(){return b<a.length?{done:!1,value:a[b++]}:{done:!0}}}function ba(a){var b="undefined"!=typeof Symbol&&Symbol.iterator&&a[Symbol.iterator];return b?b.call(a):{next:aa(a)}}function r(a){if(!(a instanceof Array)){a=ba(a);for(var b,c=[];!(b=a.next()).done;)c.push(b.value);a=c}return a}var ca="function"==typeof Object.create?Object.create:function(a){function b(){}b.prototype=a;return new b},da;if("function"==typeof Object.setPrototypeOf)da=Object.setPrototypeOf;else{var ea;a:{var fa={Fb:!0},ha={};try{ha.__proto__=fa;ea=ha.Fb;break a}catch(a){}ea=!1}da=ea?function(a,b){a.__proto__=b;if(a.__proto__!==b)throw new TypeError(a+" is not extensible");return a}:null}var ia=da;function t(a,b){a.prototype=ca(b.prototype);a.prototype.constructor=a;if(ia)ia(a,b);else for(var c in b)if("prototype"!=c)if(Object.defineProperties){var d=Object.getOwnPropertyDescriptor(b,c);d&&Object.defineProperty(a,c,d)}else a[c]=b[c]}var ja="function"==typeof Object.defineProperties?Object.defineProperty:function(a,b,c){if(a==Array.prototype||a==Object.prototype)return a;a[b]=c.value;return a};function ka(a){a=["object"==typeof globalThis&&globalThis,a,"object"==typeof window&&window,"object"==typeof self&&self,"object"==typeof global&&global];for(var b=0;b<a.length;++b){var c=a[b];if(c&&c.Math==Math)return c}throw Error("Cannot find global object");}var la=ka(this);function ma(a,b){if(b){var c=la;a=a.split(".");for(var d=0;d<a.length-1;d++){var e=a[d];e in c||(c[e]={});c=c[e]}a=a[a.length-1];d=c[a];b=b(d);b!=d&&null!=b&&ja(c,a,{configurable:!0,writable:!0,value:b})}}var na="function"==typeof Object.assign?Object.assign:function(a,b){for(var c=1;c<arguments.length;c++){var d=arguments[c];if(d)for(var e in d)Object.prototype.hasOwnProperty.call(d,e)&&(a[e]=d[e])}return a};ma("Object.assign",function(a){return a||na});ma("Math.trunc",function(a){return a?a:function(b){b=Number(b);if(isNaN(b)||Infinity===b||-Infinity===b||0===b)return b;var c=Math.floor(Math.abs(b));return 0>b?-c:c}});var u=this||self;function oa(){}function w(a){a.Pa=void 0;a.g=function(){return a.Pa?a.Pa:a.Pa=new a}}function pa(a){var b=typeof a;if("object"==b)if(a){if(a instanceof Array)return"array";if(a instanceof Object)return b;var c=Object.prototype.toString.call(a);if("[object Window]"==c)return"object";if("[object Array]"==c||"number"==typeof a.length&&"undefined"!=typeof a.splice&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("splice"))return"array";if("[object Function]"==c||"undefined"!=typeof a.call&&"undefined"!=typeof a.propertyIsEnumerable&&!a.propertyIsEnumerable("call"))return"function"}else return"null";else if("function"==b&&"undefined"==typeof a.call)return"object";return b}function qa(a){var b=pa(a);return"array"==b||"object"==b&&"number"==typeof a.length}function ra(a){return"function"==pa(a)}function sa(a){var b=typeof a;return"object"==b&&null!=a||"function"==b}function ta(a,b){var c=Array.prototype.slice.call(arguments,1);return function(){var d=c.slice();d.push.apply(d,arguments);return a.apply(this,d)}}function ua(a,b){a=a.split(".");var c=u;a[0]in c||"undefined"==typeof c.execScript||c.execScript("var "+a[0]);for(var d;a.length&&(d=a.shift());)a.length||void 0===b?c[d]&&c[d]!==Object.prototype[d]?c=c[d]:c=c[d]={}:c[d]=b}function va(a,b){function c(){}c.prototype=b.prototype;a.prototype=new c;a.prototype.constructor=a};var wa;function xa(a,b){if("string"===typeof a)return"string"!==typeof b||1!=b.length?-1:a.indexOf(b,0);for(var c=0;c<a.length;c++)if(c in a&&a[c]===b)return c;return-1}function x(a,b,c){for(var d=a.length,e="string"===typeof a?a.split(""):a,f=0;f<d;f++)f in e&&b.call(c,e[f],f,a)}function ya(a,b){for(var c=a.length,d=[],e=0,f="string"===typeof a?a.split(""):a,g=0;g<c;g++)if(g in f){var h=f[g];b.call(void 0,h,g,a)&&(d[e++]=h)}return d}function za(a,b){for(var c=a.length,d=Array(c),e="string"===typeof a?a.split(""):a,f=0;f<c;f++)f in e&&(d[f]=b.call(void 0,e[f],f,a));return d}function Aa(a,b,c){var d=c;x(a,function(e,f){d=b.call(void 0,d,e,f,a)});return d}function Ba(a,b){for(var c=a.length,d="string"===typeof a?a.split(""):a,e=0;e<c;e++)if(e in d&&b.call(void 0,d[e],e,a))return!0;return!1}function Da(a,b){var c=0;x(a,function(d,e,f){b.call(void 0,d,e,f)&&++c},void 0);return c}function Ea(a,b){b=Fa(a,b,void 0);return 0>b?null:"string"===typeof a?a.charAt(b):a[b]}function Fa(a,b,c){for(var d=a.length,e="string"===typeof a?a.split(""):a,f=0;f<d;f++)if(f in e&&b.call(c,e[f],f,a))return f;return-1}function Ga(a,b){return 0<=xa(a,b)}function Ha(a){return Array.prototype.concat.apply([],arguments)}function Ia(a){var b=a.length;if(0<b){for(var c=Array(b),d=0;d<b;d++)c[d]=a[d];return c}return[]}function Ja(a,b){a.sort(b||Ka)}function Ka(a,b){return a>b?1:a<b?-1:0}function La(a){if(!arguments.length)return[];for(var b=</td></tr>
</table>



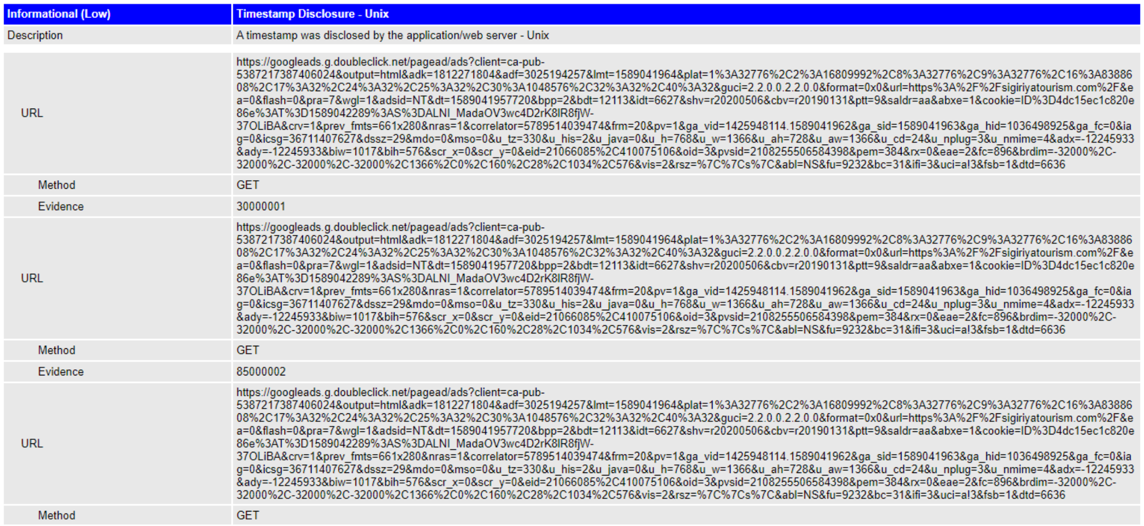
Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://partner.googleadservices.com/gampad/cookie.js?domain=sigiriyatourism.com&callback=_gfp_s_&client=ca-pub-5387217387406024
Method	GET
Evidence	1589042289
URL	https://partner.googleadservices.com/gampad/cookie.js?domain=sigiriyatourism.com&callback=_gfp_s_&client=ca-pub-5387217387406024
Method	GET
Evidence	1652114289
Instances	2
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Other information	1589042289, which evaluates to: 2020-05-09 22:08:09
Reference	https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Source ID	3



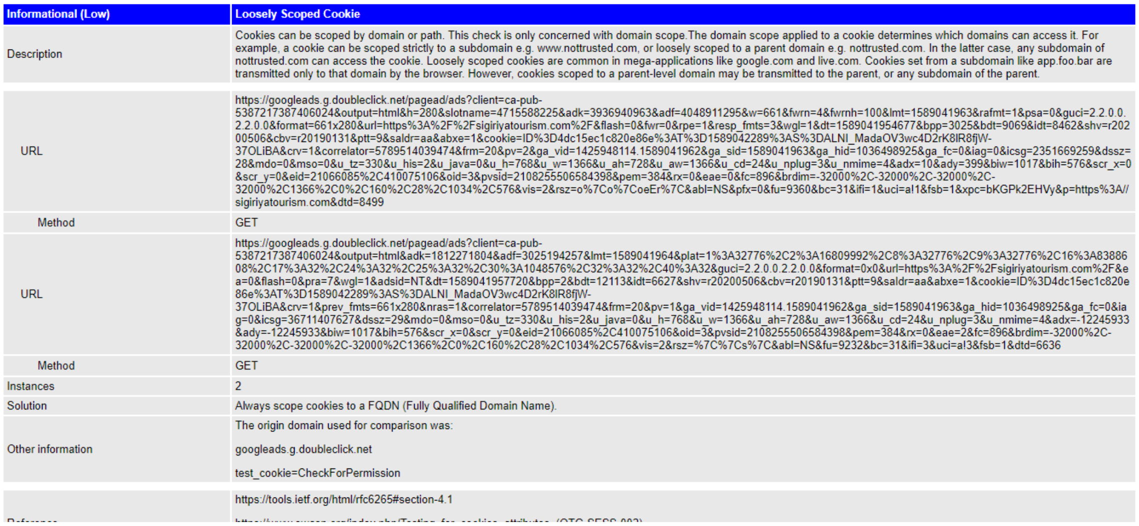
Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://www.google-analytics.com/analytics.js
Method	GET
Evidence	2147483647
URL	https://www.google-analytics.com/analytics.js
Method	GET
Evidence	268435455



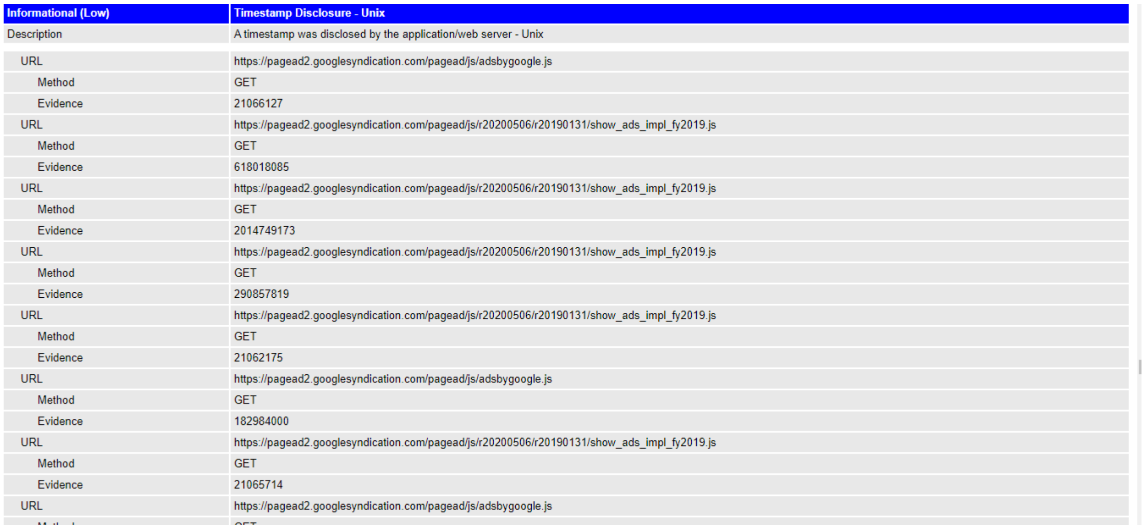
Informational (Low)	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://www.google-analytics.com/analytics.js
Method	GET
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Other information	The following comment/snippet was identified via the pattern: \bQUERY\b b));a=b;break;case "protocol":a=c;break;case "host":a=a.hostname.replace(y,"").toLowerCase();break;case "port":a=String(Number(a.port)||("http"==c?80:"https"==c?443:""));break;case "path":a.pathname||a.hostname||x();a="/"==a.pathname.substr(0,1)?a.pathname:"/"+a.pathname;a=a.split("/");a:if(b=[],c=a[a.length-1],Array.prototype.indexOf)b=b.indexOf(c),b="number"==typeof b?b:-1;else{for(var d=0;d<b.length;d++)if(b[d]===c){b=d;break a}b=-1}0<=b&&(a[a.length-1]="");a=a.join("/");break;case "query":a=a.search.replace("?", The following comment/snippet was identified via the pattern: \bQUERY\b 3988292384:d>>>1;b[c]=d}}I=b;b=4294967295;for(c=0;c<a.length;c++)b=b>>>8^I[(b^a.charCodeAt(c))&255];return((b^-1)>>>0).toString(36)},ca=function(a){return function(b){var c=B(r.location.href),d=c.search.replace("?","");a:{var f=d.split("&");for(var e=0;e<f.length;e++){var g=f[e].split("=");if("_gl"===decodeURIComponent(g[0]).replace(/\+/g," ")){f=g.slice(1).join("=");break a}}f=void 0}b.query=T(f||"")||{};f=A(c,"fragment");e=f.match(Q("_gl"));b.fragment=T(e&&e[3]||"")||{};a&&ba(c,d,f)}}; The following comment/snippet was identified via the pattern: \bQUERY\b var J=function(a){try{a:{for(var b=100;a&&0<b;){if(a.href&&a.nodeName.match(/^a(?:rea)?$/i)){var c=a;break a}a=a.parentNode;b--}c=null}if(c){var d=c.protocol;"http:"!==d&&"https:"!==d\|\|W(c,c.hostname)}}catch(f){}},K=function(a){try{if(a.action){var b=A(B(a.action),"host");W(a,b)}}catch(c){}};n("google_tag_data.glBridge.auto",function(a,b,c,d){N();c="fragment"===c?2:1;a={callback:a,domains:b,fragment:2===c,placement:c,forms:!!d,sameHost:!1};L().decorators.push(a)});n("google_tag_data.glBridge.decorate",function(a,b,c){a=S(a);return Z("_gl",a,b,!!c)});n("google_tag_data.glBridge.generate",S);n("google_tag_data.glBridge.get",function(a,b){var c=ca(!!b);b=L();b.data\|\|(b.data={query:{},fragment:{}},c(b.data));c={};if(b=b.data)p(c,b.query),a&&p(c,b.fragment);return c});})(window); The following comment/snippet was identified via the pattern: \bDB\b Ya.prototype.set=function(a,b,c){if(a)if("object"==typeof a)for(var d in a)a.hasOwnProperty(d)&&ab(this,d,a[d],c);else ab(this,a,b,c)};var ab=function(a,b,c,d){if(void 0!=c)switch(b){case Na:wb.test(c)}var e=$a(b);e&&e.o?e.o(a,b,c,d):a.data.set(b,c,d)};var ue=new ee,ve=[],bb=function(a,b,c,d,e){this.name=a;this.F=b;this.Z=d;this.o=e;this.defaultValue=c},$a=function(a){var b=ue.get(a);if(!b)for(var c=0;c<ve.length;c++){var d=ve[c],e=d[0].exec(a);if(e){b=d[1](e);ue.set(b.name,b);break}}return b},yc=function(a){var b;ue.map(function(c,d){d.F==a&&(b=d)});return b&&b.name},S=function(a,b,c,d,e){a=new bb(a,b,c,d,e);ue.set(a.name,a);return a.name},cb=function(a,b){ve.push([new RegExp("^"+a+"$"),b])},T=function(a,b,c){return S(a,b,c,void 0,db)},db=function(){};var hb=T("apiVersion","v"),ib=T("clientVersion","_v");S("anonymizeIp","aip");var jb=S("adSenseId","a"),Va=S("hitType","t"),Ia=S("hitCallback"),Ra=S("hitPayload");S("nonInteraction","ni");S("currencyCode","cu");S("dataSource","ds");var Vd=S("useBeacon",void 0,!1),fa=S("transport");S("sessionControl","sc","");S("sessionGroup","sg");S("queueTime","qt");var Ac=S("_s","_s");S("screenName","cd");var kb=S("location","dl",""),lb=S("referrer","dr"),mb=S("page","dp","");S("hostname","dh");



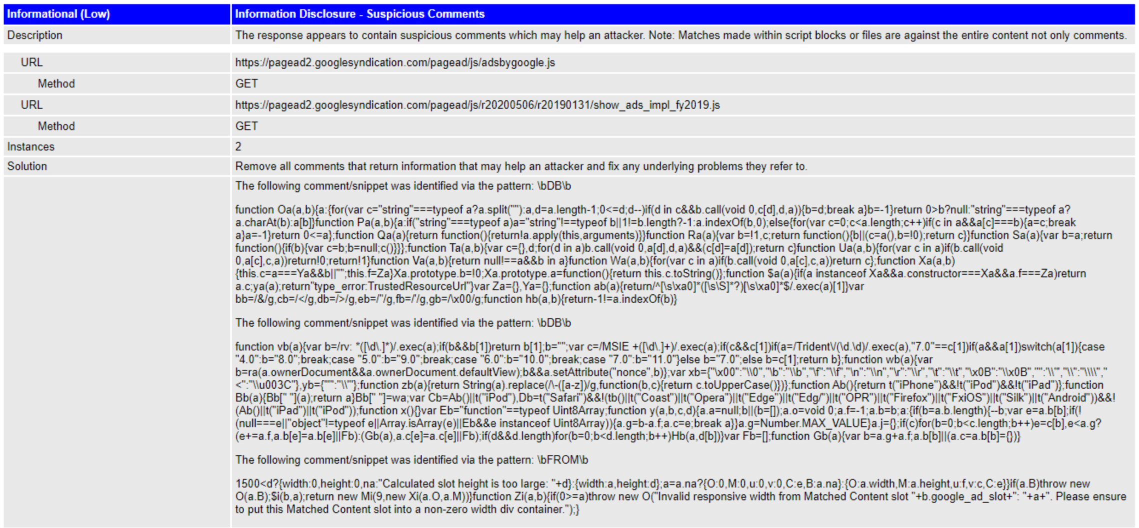
Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&adk=1812271804&adf=3025194257&lmt=1589041964&plat=1%3A32776%2C2%3A16809992%2C8%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32%2C40%3A32&guci=2.2.0.0.2.2.0.0&format=0x0&url=https%3A%2F%2Fsigiriyatourism.com%2F&ea=0&flash=0&pra=7&wgl=1&adsid=NT&dt=1589041957720&bpp=2&bdt=12113&idt=6627&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c82086e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8IR8fjW-37OLiBA&crv=1&prev_fmts=661x280&nras=1&correlator=5789514039474&frm=20&pv=1&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=36711407627&dssz=29&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=-12245933&ady=-12245933&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=2&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=%7C%7Cs%7C&abl=NS&fu=9232&bc=31&ifi=3&uci=a!3&fsb=1&dtd=6636
Method	GET
Evidence	30000001
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&adk=1812271804&adf=3025194257&lmt=1589041964&plat=1%3A32776%2C2%3A16809992%2C8%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32%2C40%3A32&guci=2.2.0.0.2.2.0.0&format=0x0&url=https%3A%2F%2Fsigiriyatourism.com%2F&ea=0&flash=0&pra=7&wgl=1&adsid=NT&dt=1589041957720&bpp=2&bdt=12113&idt=6627&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c82086e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8IR8fjW-37OLiBA&crv=1&prev_fmts=661x280&nras=1&correlator=5789514039474&frm=20&pv=1&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=36711407627&dssz=29&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=-12245933&ady=-12245933&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=2&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=%7C%7Cs%7C&abl=NS&fu=9232&bc=31&ifi=3&uci=a!3&fsb=1&dtd=6636
Method	GET
Evidence	85000002
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&adk=1812271804&adf=3025194257&lmt=1589041964&plat=1%3A32776%2C2%3A16809992%2C8%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32%2C40%3A32&guci=2.2.0.0.2.2.0.0&format=0x0&url=https%3A%2F%2Fsigiriyatourism.com%2F&ea=0&flash=0&pra=7&wgl=1&adsid=NT&dt=1589041957720&bpp=2&bdt=12113&idt=6627&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c82086e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8IR8fjW-37OLiBA&crv=1&prev_fmts=661x280&nras=1&correlator=5789514039474&frm=20&pv=1&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=36711407627&dssz=29&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=-12245933&ady=-12245933&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=2&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=%7C%7Cs%7C&abl=NS&fu=9232&bc=31&ifi=3&uci=a!3&fsb=1&dtd=6636
Method	GET



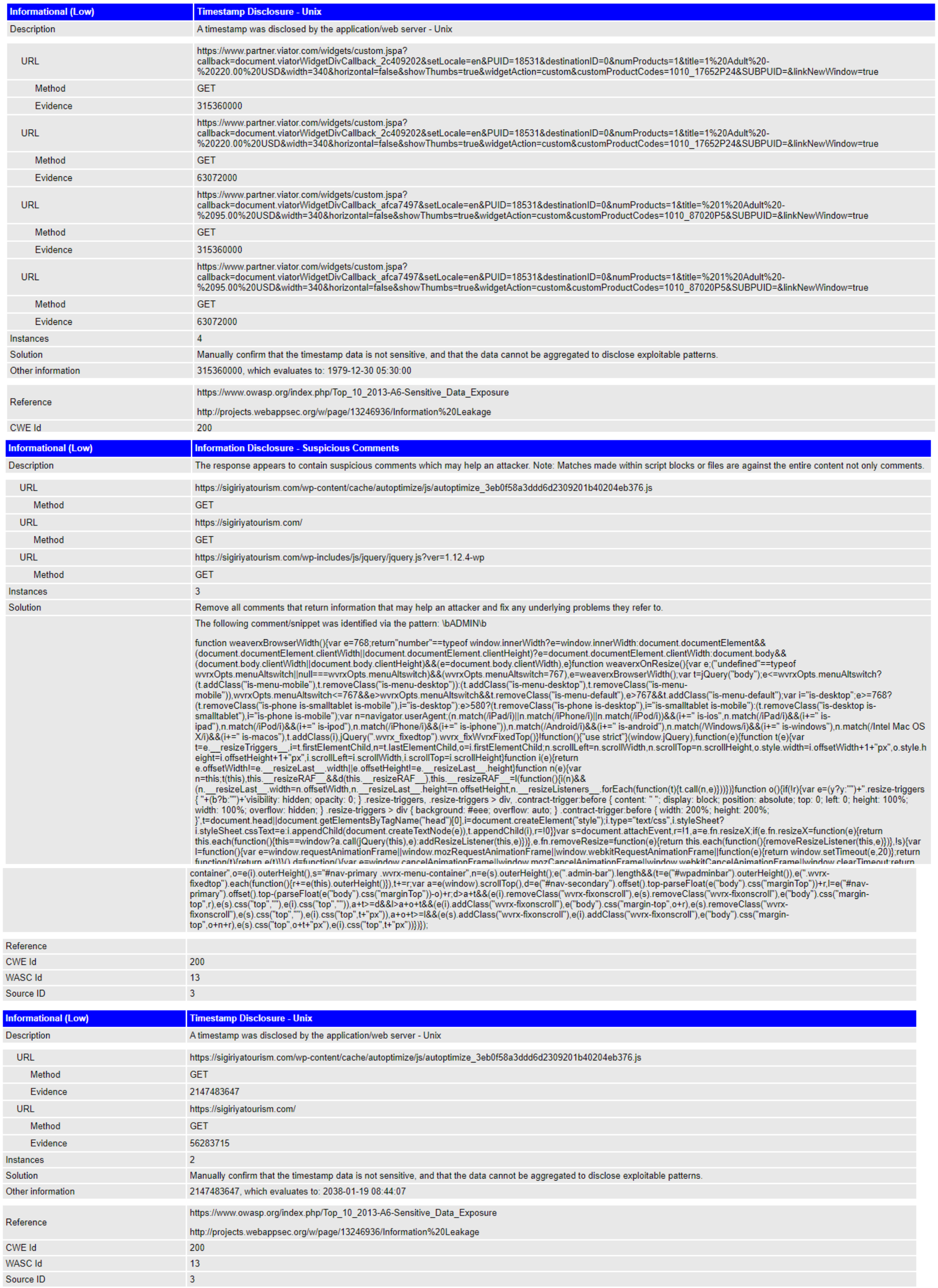
Informational (Low)	Loosely Scoped Cookie
Description	Cookies can be scoped by domain or path. This check is only concerned with domain scope.The domain scope applied to a cookie determines which domains can access it. For example, a cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. In the latter case, any subdomain of nottrusted.com can access the cookie. Loosely scoped cookies are common in mega-applications like google.com and live.com. Cookies set from a subdomain like app.foo.bar are transmitted only to that domain by the browser. However, cookies scoped to a parent-level domain may be transmitted to the parent, or any subdomain of the parent.
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&h=280&slotname=4715588225&adk=3936940963&adf=4048911295&w=661&fwrn=4&fwrnh=100&lmt=1589041963&rafmt=1&psa=0&guci=2.2.0.0.2.2.0.0&format=661x280&url=https%3A%2F%2Fsigiriyatourism.com%2F&flash=0&fwr=0&rpe=1&resp_fmts=3&wgl=1&dt=1589041954677&bpp=3025&bdt=9069&idt=8462&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c820e86e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8IR8fjW-37OLiBA&crv=1&correlator=5789514039474&frm=20&pv=2&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=2351669259&dssz=28&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=10&ady=399&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=0&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=o%7Co%7CoeEr%7C&abl=NS&pfx=0&fu=9360&bc=31&ifi=1&uci=a!1&fsb=1&xpc=bKGPk2EHVy&p=https%3A//sigiriyatourism.com&dtd=8499
Method	GET
URL	https://googleads.g.doubleclick.net/pagead/ads?client=ca-pub-5387217387406024&output=html&adk=1812271804&adf=3025194257&lmt=1589041964&plat=1%3A32776%2C2%3A16809992%2C8%3A32776%2C9%3A32776%2C16%3A8388608%2C17%3A32%2C24%3A32%2C25%3A32%2C30%3A1048576%2C32%3A32%2C40%3A32&guci=2.2.0.0.2.2.0.0&format=0x0&url=https%3A%2F%2Fsigiriyatourism.com%2F&ea=0&flash=0&pra=7&wgl=1&adsid=NT&dt=1589041957720&bpp=2&bdt=12113&idt=6627&shv=r20200506&cbv=r20190131&ptt=9&saldr=aa&abxe=1&cookie=ID%3D4dc15ec1c820e86e%3AT%3D1589042289%3AS%3DALNI_MadaOV3wc4D2rK8IR8fjW-37OLiBA&crv=1&prev_fmts=661x280&nras=1&correlator=5789514039474&frm=20&pv=1&ga_vid=1425948114.1589041962&ga_sid=1589041963&ga_hid=1036498925&ga_fc=0&iag=0&icsg=36711407627&dssz=29&mdo=0&mso=0&u_tz=330&u_his=2&u_java=0&u_h=768&u_w=1366&u_ah=728&u_aw=1366&u_cd=24&u_nplug=3&u_nmime=4&adx=-12245933&ady=-12245933&biw=1017&bih=576&scr_x=0&scr_y=0&eid=21066085%2C410075106&oid=3&pvsid=2108255506584398&pem=384&rx=0&eae=2&fc=896&brdim=-32000%2C-32000%2C-32000%2C-32000%2C1366%2C0%2C160%2C28%2C1034%2C576&vis=2&rsz=%7C%7Cs%7C&abl=NS&fu=9232&bc=31&ifi=3&uci=a!3&fsb=1&dtd=6636
Method	GET
Instances	2
Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).
Other information	The origin domain used for comparison was: googleads.g.doubleclick.net test_cookie=CheckForPermission
Reference	https://tools.ietf.org/html/rfc6265#section-4.1 https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-002)



Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Method	GET
Evidence	21066127
URL	https://pagead2.googlesyndication.com/pagead/js/r20200506/r20190131/show_ads_impl_fy2019.js
Method	GET
Evidence	618018085
URL	https://pagead2.googlesyndication.com/pagead/js/r20200506/r20190131/show_ads_impl_fy2019.js
Method	GET
Evidence	2014749173
URL	https://pagead2.googlesyndication.com/pagead/js/r20200506/r20190131/show_ads_impl_fy2019.js
Method	GET
Evidence	290857819
URL	https://pagead2.googlesyndication.com/pagead/js/r20200506/r20190131/show_ads_impl_fy2019.js
Method	GET
Evidence	21062175
URL	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Method	GET
Evidence	182984000
URL	https://pagead2.googlesyndication.com/pagead/js/r20200506/r20190131/show_ads_impl_fy2019.js
Method	GET
Evidence	21065714
URL	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Method	GET



Informational (Low)	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js
Method	GET
URL	https://pagead2.googlesyndication.com/pagead/js/r20200506/r20190131/show_ads_impl_fy2019.js
Method	GET
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
	The following comment/snippet was identified via the pattern: \bDB\b function Oa(a,b){a:{for(var c="string"===typeof a?a.split(""):a,d=a.length-1;0<=d;d--)if(d in c&&b.call(void 0,c[d],d,a)){b=d;break a}b=-1}return 0>b?null:"string"===typeof a?a.charAt(b):a[b]}function Pa(a,b){a:if("string"===typeof a)a="string"!==typeof b||1!=b.length?-1:a.indexOf(b,0);else{for(var c=0;c<a.length;c++)if(c in a&&a[c]===b){a=c;break a}a=-1}return 0<=a};function Qa(a){return function(){return!a.apply(this,arguments)}}function Ra(a){var b=!1,c;return function(){b||(c=a(),b=!0);return c}}function Sa(a){var b=a;return function(){if(b){var c=b;b=null;c()}}};function Ta(a,b){var c={},d;for(d in a)b.call(void 0,a[d],d,a)&&(c[d]=a[d]);return c}function Ua(a,b){for(var c in a)if(b.call(void 0,a[c],c,a))return!0;return!1}function Va(a,b){return null!==a&&b in a}function Wa(a,b){for(var c in a)if(b.call(void 0,a[c],c,a))return c};function Xa(a,b){this.c=a===Ya&&b||"";this.f=Za}Xa.prototype.b=!0;Xa.prototype.a=function(){return this.c.toString()};function $a(a){if(a instanceof Xa&&a.constructor===Xa&&a.f===Za)return a.c;ya(a);return"type_error:TrustedResourceUrl"}var Za={},Ya={};function ab(a){return/^[\s\xa0]*([\s\S]*?)[\s\xa0]*$/.exec(a)[1]}var bb=/&/g,cb=/</g,db=/>/g,eb=/"/g,fb=/'/g,gb=/\x00/g;function hb(a,b){return-1!=a.indexOf(b)} The following comment/snippet was identified via the pattern: \bDB\b function vb(a){var b=/rv: *([\d\.]*)/.exec(a);if(b&&b[1])return b[1];b="";var c=/MSIE +([\d\.]+)/.exec(a);if(c&&c[1])if(a=/Trident\/(\d.\d)/.exec(a),"7.0"==c[1])if(a&&a[1])switch(a[1]){case "4.0":b="8.0";break;case "5.0":b="9.0";break;case "6.0":b="10.0";break;case "7.0":b="11.0"}else b="7.0";else b=c[1];return b};function wb(a){var b=ra(a.ownerDocument&&a.ownerDocument.defaultView);b&&a.setAttribute("nonce",b)};var xb={"\x00":"\\0","\b":"\\b","\f":"\\f","\n":"\\n","\r":"\\r","\t":"\\t","\x0B":"\\x0B",'"':'\\"',"\\":"\\\\","<":"\\u003C"},yb={"'":"\\'"};function zb(a){return String(a).replace(/\-([a-z])/g,function(b,c){return c.toUpperCase()})};function Ab(){return t("iPhone")&&!t("iPod")&&!t("iPad")};function Bb(a){Bb[" "](a);return a}Bb[" "]=wa;var Cb=Ab()||t("iPod"),Db=t("Safari")&&!(tb()||t("Coast")||t("Opera")||t("Edge")||t("Edg/")||t("OPR")||t("Firefox")||t("FxiOS")||t("Silk")||t("Android"))&&!(Ab()||t("iPad")||t("iPod"));function x(){}var Eb="function"==typeof Uint8Array;function y(a,b,c,d){a.a=null;b||(b=[]);a.o=void 0;a.f=-1;a.b=b;a:{if(b=a.b.length){--b;var e=a.b[b];if(!(null===e||"object"!=typeof e||Array.isArray(e)||Eb&&e instanceof Uint8Array)){a.g=b-a.f;a.c=e;break a}}a.g=Number.MAX_VALUE}a.j={};if(c)for(b=0;b<c.length;b++)e=c[b],e<a.g?(e+=a.f,a.b[e]=a.b[e]||Fb):(Gb(a),a.c[e]=a.c[e]||Fb);if(d&&d.length)for(b=0;b<d.length;b++)Hb(a,d[b])}var Fb=[];function Gb(a){var b=a.g+a.f;a.b[b]||(a.c=a.b[b]={})} The following comment/snippet was identified via the pattern: \bFROM\b 1500<d?{width:0,height:0,na:"Calculated slot height is too large: "+d}:{width:a,height:d};a=a.na?{O:0,M:0,u:0,v:0,C:e,B:a.na}:{O:a.width,M:a.height,u:f,v:c,C:e}}if(a.B)throw new O(a.B);$i(b,a);return new Mi(9,new Xi(a.O,a.M))}function Zi(a,b){if(0>=a)throw new O("Invalid responsive width from Matched Content slot "+b.google_ad_slot+": "+a+". Please ensure to put this Matched Content slot into a non-zero width div container.");}



Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Evidence	315360000
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_2c409202&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=1%20Adult%20-%20220.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_17652P24&SUBPUID=&linkNewWindow=true
Method	GET
Evidence	63072000
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Method	GET
Evidence	315360000
URL	https://www.partner.viator.com/widgets/custom.jspa?callback=document.viatorWidgetDivCallback_afca7497&setLocale=en&PUID=18531&destinationID=0&numProducts=1&title=%201%20Adult%20-%2095.00%20USD&width=340&horizontal=false&showThumbs=true&widgetAction=custom&customProductCodes=1010_87020P5&SUBPUID=&linkNewWindow=true
Method	GET
Evidence	63072000
Instances	4
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Other information	315360000, which evaluates to: 1979-12-30 05:30:00
Reference	https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200

Informational (Low)	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://sigiriyatourism.com/wp-content/cache/autoptimize/js/autoptimize_3eb0f58a3ddd6d2309201b40204eb376.js
Method	GET
URL	https://sigiriyatourism.com/
Method	GET
URL	https://sigiriyatourism.com/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp
Method	GET
Instances	3
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

The following comment/snippet was identified via the pattern: \bADMIN\b

```
function weaverxBrowserWidth(){var e=768;return"number"==typeof window.innerWidth?e=window.innerWidth:document.documentElement&&
(document.documentElement.clientWidth||document.documentElement.clientHeight)?e=document.documentElement.clientWidth:document.body&&
(document.body.clientWidth||document.body.clientHeight)&&(e=document.body.clientWidth),e}function weaverxOnResize(){var e;("undefined"==typeof
wvrxOpts.menuAltswitch||null===wvrxOpts.menuAltswitch)&&(wvrxOpts.menuAltswitch=767),e=weaverxBrowserWidth();var t=jQuery("body");e<=wvrxOpts.menuAltswitch?
(t.addClass("is-menu-mobile"),t.removeClass("is-menu-desktop")):(t.addClass("is-menu-desktop"),t.removeClass("is-menu-
mobile")),wvrxOpts.menuAltswitch<=767&&e>wvrxOpts.menuAltswitch&&t.removeClass("is-menu-default"),e>767&&t.addClass("is-menu-default");var i="is-desktop";e>=768?
(t.removeClass("is-phone is-smalltablet is-mobile"),i="is-desktop"):e>580?(t.removeClass("is-phone is-desktop"),i="is-smalltablet is-mobile"):(t.removeClass("is-desktop is-
smalltablet"),i="is-phone is-mobile");var n=navigator.userAgent;(n.match(/iPad/i)||n.match(/iPhone/i)||n.match(/iPod/i))&&(i+=" is-ios",n.match(/iPad/i)&&(i+=" is-
ipad"),n.match(/iPod/i)&&(i+=" is-ipod"),n.match(/iPhone/i)&&(i+=" is-iphone")),n.match(/Android/i)&&(i+=" is-android"),n.match(/Windows/i)&&(i+=" is-windows"),n.match(/Intel Mac OS
X/i)&&(i+=" is-macos"),t.addClass(i),jQuery(".wvrx_fixedtop").wvrx_fixWvrxFixedTop()}!function(){"use strict"}(window.jQuery),function(e){function t(e){var
t=e.__resizeTriggers__,i=t.firstElementChild,n=t.lastElementChild,o=i.firstElementChild;n.scrollLeft=n.scrollWidth,n.scrollTop=n.scrollHeight,o.style.width=i.offsetWidth+1+"px",o.style.h
eight=i.offsetHeight+1+"px",i.scrollLeft=i.scrollWidth,i.scrollTop=i.scrollHeight}function i(e){return
e.offsetWidth!=e.__resizeLast__.width||e.offsetHeight!=e.__resizeLast__.height}function n(e){var
n=this;t(this),this.__resizeRAF__&&d(this.__resizeRAF__),this.__resizeRAF__=l(function(){i(n)&&
(n.__resizeLast__.width=n.offsetWidth,n.__resizeLast__.height=n.offsetHeight,n.__resizeListeners__.forEach(function(t){t.call(n,e)}))})}function o(){if(!r){var e=(y?y:"")+".resize-triggers
{ "+(b?b:"")+'visibility: hidden; opacity: 0; } .resize-triggers, .resize-triggers > div, .contract-trigger:before { content: " "; display: block; position: absolute; top: 0; left: 0; height: 100%;
width: 100%; overflow: hidden; } .resize-triggers > div { background: #eee; overflow: auto; } .contract-trigger:before { width: 200%; height: 200%;
}',t=document.head||document.getElementsByTagName("head")[0],i=document.createElement("style");i.type="text/css",i.styleSheet?
i.styleSheet.cssText=e:i.appendChild(document.createTextNode(e)),t.appendChild(i),r=!0}}var s=document.attachEvent,r=!1,a=e.fn.resizeX;if(e.fn.resizeX=function(e){return
this.each(function(){this==window?a.call(jQuery(this),e):addResizeListener(this,e)})},e.fn.removeResize=function(e){return this.each(function(){removeResizeListener(this,e)})},!s){var
l=function(){var e=window.requestAnimationFrame||window.mozRequestAnimationFrame||window.webkitRequestAnimationFrame||function(e){return window.setTimeout(e,20)};return
function(t){return e(t)}}(),d=function(){var e=window.cancelAnimationFrame||window.mozCancelAnimationFrame||window.webkitCancelAnimationFrame||window.clearTimeout;return
container",o=e(i).outerHeight(),s="#nav-primary .wvrx-menu-container",n=e(s).outerHeight();e(".admin-bar").length&&(t=e("#wpadminbar").outerHeight()),e(".wvrx-
fixedtop").each(function(){r+=e(this).outerHeight()}),t+=r;var a=e(window).scrollTop(),d=e("#nav-secondary").offset().top-parseFloat(e("body").css("marginTop"))+r,l=e("#nav-
primary").offset().top-(parseFloat(e("body").css("marginTop"))-o)+r;d>a+t&&(e(i).removeClass("wvrx-fixonscroll"),e(s).removeClass("wvrx-fixonscroll"),e("body").css("margin-
top",r),e(s).css("top",""),e(i).css("top","")),a+t>=d&&l>a+o+t&&(e(i).addClass("wvrx-fixonscroll"),e("body").css("margin-top",o+r),e(s).removeClass("wvrx-
fixonscroll"),e(s).css("top",""),e(i).css("top",t+"px")),a+o+t>=l&&(e(s).addClass("wvrx-fixonscroll"),e(i).addClass("wvrx-fixonscroll"),e("body").css("margin-
top",o+n+r),e(s).css("top",o+t+"px"),e(i).css("top",t+"px"))}})});
```

Reference	
CWE Id	200
WASC Id	13
Source ID	3

Informational (Low)	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://sigiriyatourism.com/wp-content/cache/autoptimize/js/autoptimize_3eb0f58a3ddd6d2309201b40204eb376.js
Method	GET
Evidence	2147483647
URL	https://sigiriyatourism.com/
Method	GET
Evidence	56283715
Instances	2
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Other information	2147483647, which evaluates to: 2038-01-19 08:44:07
Reference	https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Source ID	3

Fig 4.9 : scan report

5. Conclusion

In these audits, we can identify what kind of weakness that is on our website and what is are solutions to those issues. The audit report has this issue divided to as risk level. We can, after doing these solutions, again scan our website use ZAP tools. We will show any problems has our web site anymore.

6. REFERENCES

[1] https://www.cloudflare.com/learning/security/what-is-web-application-security/

[2] https://dzone.com/articles/top-10-automated-software-testing-tools

[3] https://www.imperva.com/learn/application-security/application-security/