Report

1).Findings:

The site Zero Bank Of url:http://zero.webappsecurity.com/ is vulnerable to some major extent. In our vulnerability assessment of the domain, we have found about 24 vulnerabilities from zap tool ranging from severity of high to some informational category of vulnerabilities.

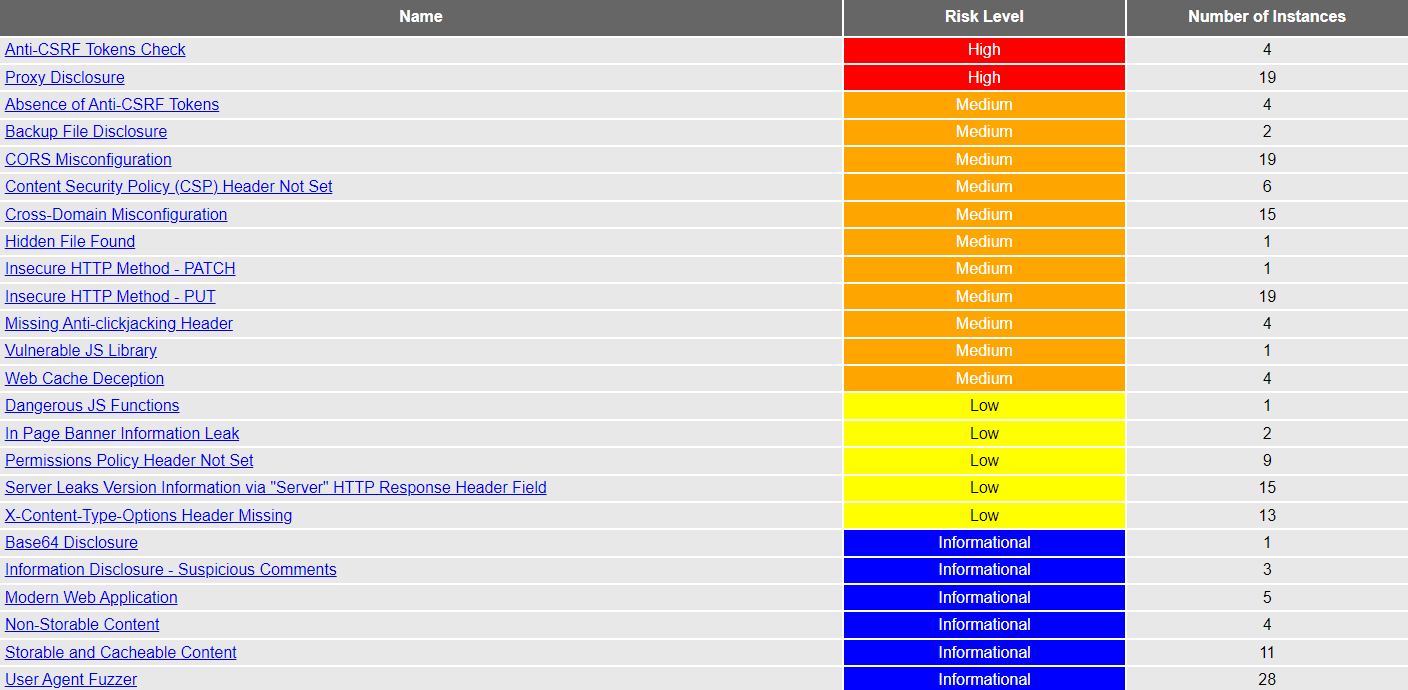
2).Risk Assessment:

High: 2

Medium: 11

Low: 5

Informational: 6



3).High Severity Vulnerability:

Name : Anti-CSRF Tokens Check

Impact:

A Cross site request forgery is an attack in which a victim sends an HTTP request to target destination without their knowledge and it is performed with an intent to attack the destination url as a valid user. The use is of using the predictable syntax of URL/form actions in a repetable way. In this CSRF exploits the trust that a website has for user in which an attacker analyzes the html code or the syntax of the commands, html and php an manipulates it in order to exploit this vulnerability. CSRF attacks are not necessarily cross-site but it 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:

1.The victim has an active session on the target site.

2.The victim is authenticated via HTTP auth on the target site.

3.The victim is on the same local network as the target

4).Instances:

There has been 4 instances where the high severity vulnerability have been detected in the site of the Zero Bank.

1.) URL: http://zero.webappsecurity.com

Method: GET

Evidence : <form action="/search.html" class="navbar-search pull-right" style="padding-right:20px">

2.) URL: http://zero.webappsecurity.com/

Method: GET

Evidence : <form action="/search.html" class="navbar-search pull-right" style="padding-right:20px">

3.) URL: http://zero.webappsecurity.com/index.html

Method: GET

Evidence : <form action="/search.html" class="navbar-search pull-right" style="padding-right:20px">

4.) URL: http://zero.webappsecurity.com/search.html?searchTerm=ZAP

Method: GET

Evidence : <form action="/search.html" class="navbar-search pull-right" style="padding-right:20px">

CWE id : 352

Tags: OWASP\_2021\_A05, WSTG-v42-SESS-05, OWASP\_2017\_A06

Reference : http://projects.webappsec.org/Cross-Site-Request-Forgery

<http://cwe.mitre.org/data/definitions/352.html>

5).Solution:

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to exploit the system and also remediates the problem.

eg:use anti-CSRF packages like OWASP CSRFGuard

Phase: Implementation

Ensure the implementation of code free of cross-site scripting issues.

Phase: Architecture and Design

Do not use GET method for any requests that triggers a state change.