Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by HCL AppScan Standard 10.4.0
Scan started: 6/7/2024 5:59:42 PM

Table of Contents

Introduction

This report contains the results of a web application security scan performed by HCL AppScan Standard.

Medium severity issues:	2
Total security issues included in the report:	2
Total security issues discovered in the scan:	52

General Information

Scan file name:	swik.meity.gov.in_eSignUser
Scan started:	6/7/2024 5:59:42 PM
Test policy:	Default
CVSS version:	3.1
Test optimization level:	Fast

Host	10.246.140.36
Port	80
Operating system:	Unknown
Web server:	Unknown
Application server:	Any

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
In-session detection:	Enabled
In-session pattern:	`Approval\ Letter\ Pending\ for\ Signature|Signed\ Approved\ Proposals|Update\ Profile`
Tracked or session ID cookies:	`aadhaar_good_governance_portal_session` `XSRF-TOKEN`
Tracked or session ID parameters:	`_token` `_token`

Login sequence:	`http://10.246.140.36/`
	`http://10.246.140.36/login`
	`http://10.246.140.36/login`
	`http://10.246.140.36/home`
	`http://10.246.140.36/2fa`

```
http://10.246.140.36/2fa
http://10.246.140.36/home
```

Summary

Issue Types 2

TOC

	Issue Type	Number of Issues
M	Integer Overflow	1
M	Unnecessary Http Response Headers found in the Application	1

Vulnerable URLs 2

TOC

	URL	Number of Issues
M	http://10.246.140.36/userValidate	1
M	http://10.246.140.36/js/jquery-3.7.1.min.js	1

Fix Recommendations 2

TOC

	Remediation Task	Number of Issues
M	Do not allow sensitive information to leak.	1
M	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	1

Security Risks 2

TOC

	Risk	Number of Issues
M	It is possible to gather sensitive debugging information	1
M	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	1

Causes 2

TOC

	Cause	Number of Issues
M	An Integer Overflow (or wraparound) occurs when a value that is too large is stored (larger than the maximum value the variable can hold) in an integer data type (including byte, short, long, and other types). The most significant bits of the integer are lost, and the remaining value is relative to the minimum value (either 0 or very negative value for signed types).	1
M	Insecure web application programming or configuration	1

WASC Threat Classification

TOC

Threat	Number of Issues
Information Leakage	1
Integer Overflows	1

Issues Sorted by Issue Type

M Integer Overflow 1 TOC

Issue 1 of 1 TOC

Integer Overflow

Severity:	Medium
CVSS Score:	8.6
URL:	http://10.246.140.36/userValidate
Entity:	mobile (Parameter)
Risk:	It is possible to gather sensitive debugging information
Cause:	An Integer Overflow (or wraparound) occurs when a value that is too large is stored (larger than the maximum value the variable can hold) in an integer data type (including byte, short, long, and other types). The most significant bits of the integer are lost, and the remaining value is relative to the minimum value (either 0 or very negative value for signed types).
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
GET /userValidate?mobile=9999999999999999999&validation_type=mobile&id=0 HTTP/1.1
Host: 10.246.140.36
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
_token: {{ csrf_token() }}
Accept-Language: en-US
Connection: keep-alive
Cookie:
aadhaar_good_governance_portal_session=eyJpdiI6InJhV3M2T1BxS1JqOGwyR2ZsQS8yV2c9PSIsInZhbHVlIjoiUGZhOVYxY2pheWt3ZWptRU1NSjhR
Q1dzbW5UcXoxS1pIb3JCYjRlVWVoRGs4NHZ5SEZvcktFQWVpd0ZSTk1vQWU3SkZ2bGVjRlhES1FRVFloZzczY2xLcGt2ZmVOcnU3T3FESUJzRWNqNU4rZVFOL0R
TR3gzVWg4T1RJNmpyL0UiLCJtYWMiOiJhMzk5MDUwMWFkZDM4OGJjNzQ5MGUwNjIyMGY0MjlkZWEzMGYyMDZmYWIwOTA2ODYxOGU0YmQwZTdmZTYxOTczIiwidG
FnIjoiIn0%3D
Content-Length: 0


HTTP/1.1 500 Internal Server Error
Date: Fri, 07 Jun 2024 12:35:23 GMT
Server: Swik
Cache-Control: must-revalidate, no-cache, no-store, private
Pragma: no-cache
X-Frame-Options: SAMEORIGIN, SAMEORIGIN
Content-Security-Policy: default-src 'self';Object-Src 'self'; img-src  'self' data:; script-src 'self'; style-src 'self'
'unsafe-inline';
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
```

```
X-XSS-Protection: 1; mode=block
X-Firefox-Spdy: h2
Strict-Transport-Security: max-age=31536000; includeSubDomains
Access-Control-Allow-Methods: GET, POST, HEAD
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: accept, content-type, X-Requested-With, X-Prototype-Version, X-CSRF-Token, authorization
Referrer-Policy: no-referrer
Connection: close
Transfer-Encoding: chunked
Content-Type: application/json
Set-Cookie: XSRF-
TOKEN=eyJpdiI6IjJERldZQXpwT09RVTRzRmphOFV6Qmc9PSIsInZhbHVlIjoiemZ3aVFjOXJwNEY5bUJ0dURYdlFJb1YwMmdONi9EdXJFWlV3R3hrSWU3dXRPN
0lNYWdkZDVDZkcyTGlHSDA0TCIsIm1hYyI6IjgzM2FkYmQxN2Q4OWQwMDAwY2JjMTY1YTIyNmRlM2M4Y2VjYWNmNGZkZWRmZDBjNTQwYzVhOTY3M2ZlMGUyY2Ui
LCJ0YWciOiIifQ==; expires=Fri, 07-Jun-2024 13:35:23 GMT; Max-Age=3600; path=/; secure; httponly; samesite=strict
Set-Cookie:
aadhaar_good_governance_portal_session=eyJpdiI6ImpvMmpoRHBVd05EZElEUlRsS0E2SHc9PSIsInZhbHVlIjoicHhJWG9ScitHczVGSjVlbVJWR0Qr
UFQ1bDJvY05wc2NveSt4clVjdjltMk1qTVhOUGN3QkVTZyttdHdwVDcwY2dJV1M5NkNHZHp1Wk1HZE01MGEwM0JMbXZRVFlycVV2K3Fha3ZUKzljN3hnSGVhZDF
IdTJtbVdKTWN5WnhlUk4iLCJtYWMiOiI0NDI2OWI5ODM0MDdhNjNlYjczMGIyMTk3M2E1MTU4ZGFlMDRkMGNkMzQxOGU3MWNjMzFlNTc3NzBkNTk5NDE1IiwidG
FnIjoiIn0%3D; path=/; httponly; samesite=strict

{

"message": "Server Error"

}
```

M Unnecessary Http Response Headers found in the Application 1 TOC

Issue 1 of 1 TOC

Unnecessary Http Response Headers found in the Application

Severity:	Medium
CVSS Score:	3.7
URL:	http://10.246.140.36/js/jquery-3.7.1.min.js
Entity:	10.246.140.36 (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Do not allow sensitive information to leak.

Reasoning: The response contains unnecessary headers, which may help attackers in planning further attacks.

Test Requests and Responses:

```
GET /js/jquery-3.7.1.min.js HTTP/1.1
Host: 10.246.140.36
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept: */*
Accept-Language: en-US
Connection: keep-alive
Cookie:
aadhaar_good_governance_portal_session=eyJpdiI6Imx4di9kdnRvZkRBSWlUOURhOEI1RXc9PSIsInZhbHVlIjoicGVDSkNDYlJzRUY4dCtGUCt2SWRk
OWNTalpnQVhOcXlwS1Vlak5VcDVtRWlvWW5lRnZBaytOMGI5ZzEyNDhVTUNlTVdNTExiNkVuandscTVLTWdQRzVNb2swN2RGbGtSeUdycTNabTEwY0V3N2JUY1J
vdzZJMEFJRUxoeStyRmoiLCJtYWMiOiIwOWY1MmVkMTYzMWEzYmM4OWNjNGU4NDhlYjc5OGU4MjExYWE1YWFjNzA4NWU4NGVlNWUxMDJkMjI4NDMwMzc0IiwidG
FnIjoiIn0%3D
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Fri, 07 Jun 2024 12:34:05 GMT
Server: Swik
X-Frame-Options: SAMEORIGIN, SAMEORIGIN
Content-Security-Policy: default-src 'self';Object-Src 'self'; img-src  'self' data:; script-src 'self'; style-src 'self'
'unsafe-inline';
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Last-Modified: Fri, 15 Dec 2023 05:20:54 GMT
Accept-Ranges: bytes
Content-Length: 87532
X-XSS-Protection: 1; mode=block
X-Firefox-Spdy: h2
Strict-Transport-Security: max-age=31536000; includeSubDomains
Access-Control-Allow-Methods: GET, POST, HEAD
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: accept, content-type, X-Requested-With, X-Prototype-Version, X-CSRF-Token, authorization
Referrer-Policy: no-referrer
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/javascript

/*! jQuery v3.7.1 | (c) OpenJS Foundation and other contributors | jquery.org/license */
!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?
t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}
("undefined"!=typeof window?window:this,function(ie,e){"use strict";var oe=
[],r=Object.getPrototypeOf,ae=oe.slice,g=oe.flat?function(e){return oe.flat.call(e)}:function(e){return
oe.concat.apply([],e)},s=oe.push,se=oe.indexOf,n={},i=n.toString,ue=n.hasOwnProperty,o=ue.toString,a=o.call(Object),le=
{},v=function(e){return"function"==typeof e&&"number"!=typeof e.nodeType&&"function"!=typeof e.item},y=function(e){return
null!=e&&e===e.window},C=ie.document,u={type:!0,src:!0,nonce:!0,noModule:!0};function m(e,t,n){var r,i,o=
(n=n||C).createElement("script");if(o.text=e,t)for(r in u)
(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNode.removeChild(o)}function
x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?n[i.call(e)]||"object":typeof e}var
t="3.7.1",l=/HTML$/i,ce=function(e,t){return new ce.fn.init(e,t)};function c(e){var t=!!e&&"length"in
e&&e.length,n=x(e);return!v(e)&&!y(e)&&("array"===n||0===t||"number"==typeof t&&0<t&&t-1 in e)}function fe(e,t){return
e.nodeName&&e.nodeName.toLowerCase()===t.toLowerCase()}ce.fn=ce.prototype=
{jquery:t,constructor:ce,length:0,toArray:function(){return ae.call(this)},get:function(e){return null==e?
ae.call(this):e<0?this[e+this.length]:this[e]},pushStack:function(e){var t=ce.merge(this.constructor(),e);return
t.prevObject=this,t},each:function(e){return ce.each(this,e)},map:function(n){return
this.pushStack(ce.map(this,function(e,t){return n.call(e,t,e)}))},slice:function(){return
this.pushStack(ae.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-
1)},even:function(){return this.pushStack(ce.grep(this,function(e,t){return(t+1)%2}))},odd:function(){return
this.pushStack(ce.grep(this,function(e,t){return t%2}))},eq:function(e){var t=this.length,n=+e+(e<0?t:0);return
this.pushStack(0<=n&&n<t?[this[n]]:[])},end:function(){return
this.prevObject||this.constructor()},push:s,sort:oe.sort,splice:oe.splice},ce.extend=ce.fn.extend=function(){var
e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.length,l=!1;for("boolean"==typeof a&&(l=a,a=arguments[s]||
{},s++),"object"==typeof a||v(a)||(a={}),s===u&&(a=this,s--);s<u;s++)if(null!=(e=arguments[s]))for(t in
e)r=e[t],"__proto__"!==t&&a!==r&&(l&&r&&(ce.isPlainObject(r)||(i=Array.isArray(r)))?(n=a[t],o=i&&!Array.isArray(n)?
[]:i||ce.isPlainObject(n)?n:{},i=!1,a[t]=ce.extend(l,o,r)):void 0!==r&&(a[t]=r));return a},ce.extend({expando:"jQuery"+
(t+Math.random()).replace(/\D/g,""),isReady:!0,error:function(e){throw new Error(e)},noop:function()
{},isPlainObject:function(e){var t,n;return!(!e||"[object Object]"!==i.call(e))&&(!
(t=r(e))||"function"==typeof(n=ue.call(t,"constructor")&&t.constructor)&&o.call(n)===a)},isEmptyObject:function(e){var
t;for(t in e)return!1;return!0},globalEval:function(e,t,n){m(e,{nonce:t&&t.nonce},n)},each:function(e,t){var n,r=0;if(c(e))
{for(n=e.length;r<n;r++)if(!1===t.call(e[r],r,e[r]))break}else for(r in e)if(!1===t.call(e[r],r,e[r]))break;return
e},text:function(e){var t,n="",r=0,i=e.nodeType;if(!i)while(t=e[r++])n+=ce.text(t);return 1===i||11===i?
e.textContent:9===i?e.documentElement.te
...
...
...
```

How to Fix

Integer Overflow

TOC

Cause:

An Integer Overflow (or wraparound) occurs when a value that is too large is stored (larger than the maximum value the variable can hold) in an integer data type (including byte, short, long, and other types). The most significant bits of the integer are lost, and the remaining value is relative to the minimum value (either 0 or very negative value for signed types).

Risk:

When an integer overflow occurs, the interpreted value will appear to have 'wrapped around' past the maximum value and reset back to the minimum value.
The value can unexpectedly become zero or negative. This can have security implications if the value is used to control looping, manage resources (such as memory allocation), or make business logic decisions.
For example, an integer overflow can give money to the customer in addition to their purchases, when the transaction is completed.
In particular, if a mathematical operation results in a number larger than the maximum possible for the integer type, the value wraps around and the variable is set to zero, or negative.
i=UINT_MAX+1; // Maximum value for a variable of type unsigned int - 4294967295 (0xffffffff). The result is: i=0

Fix Recommendation:

General

Validate all inputs are within an expected range and the sign before relying on their values or using them in arithmetic calculations.
Be sure to check both upper bounds and lower bounds, including negative lower bounds for signed integers (integer overflow is also possible with very large negative numbers).
Use unsigned integers where possible.
Consider using a safe integer-handling library (such as C/C++ SafeInt or IntegerLib).
Consider enabling compiler extensions that prevent some classes of buffer overflows.

CWE:

190

External References:

SafeInt Library

Unnecessary Http Response Headers found in the Application

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web server type, version, OS and more.
AppScan detected a Http response header that is unnecessary.
For reasons of security and privacy, The Http response headers like "Server", "X-Powered-By", "X-AspNetMvc-Version" and "X-AspNet-Version" should not appear in web pages.
The "Server" header is a header that is added usually by default whenever a response is sent to the client by the server.
The "X-Powered-By" header is a header that might be added by default whenever a response is sent to the client by the server.
These added header(s) may reveal sensitive information about the internal server software version and type, thus enabling attackers to fingerprint it and attack it with targeted exploits. Moreover, when a new exploit becomes known to the public, the server will most likely get attacked with it.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Configure your server to remove the default "Server" header from being sent to all outgoing requests.
For IIS, see:
https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710
For nginx, see:
https://www.getpagespeed.com/server-setup/nginx/how-to-remove-the-server-header-in-nginx
For Weblogic, see:
https://docs.oracle.com/cd/E13222_01/wls/docs81/adminguide/web_server.html
For Apache, see:
https://techglimpse.com/set-modify-response-headers-http-tip/

CWE:

200

External References:

Fingerprinting
Preventing Information Leakage

Application Data

Visited URLs 102

TOC

URL
http://10.246.140.36/
http://10.246.140.36/login
http://10.246.140.36/js/jquery-3.7.1.min.js
http://10.246.140.36/js/datatable.js
http://10.246.140.36/vendor/bootstrap/js/bootstrap.min.js
http://10.246.140.36/js/script.js?v=1717763418
http://10.246.140.36/js/script.js?v=1717763394
http://10.246.140.36/profile
http://10.246.140.36/js/jquery.validate.min.js
http://10.246.140.36/vendor/select2/select2.min.js
http://10.246.140.36/vendor/bootstrap/js/bootstrap-select.min.js
http://10.246.140.36/js/forge.min.js
http://10.246.140.36/js/login.js
http://10.246.140.36/
http://10.246.140.36/js/script.js?v=1717763397
http://10.246.140.36/login
http://10.246.140.36/home
http://10.246.140.36/2fa
http://10.246.140.36/js/script.js?v=1717763400
http://10.246.140.36/js/script.js?v=1717763419
http://10.246.140.36/2fa
http://10.246.140.36/js/script.js?v=1717763402
http://10.246.140.36/vendor/bootstrap/js/popper.min.js
http://10.246.140.36/js/script.js?v=1717763408
http://10.246.140.36/proposals/upload-sign
http://10.246.140.36/js/script.js?v=1717763410
http://10.246.140.36/js/script.js?v=1717763422
http://10.246.140.36/js/attachment-preview.js
http://10.246.140.36/js/script.js?v=1717763415
http://10.246.140.36/proposals/accepted
http://10.246.140.36/js/script.js?v=1717763417
http://10.246.140.36/js/proposal-accept.js
http://10.246.140.36/js/profile-update.js
http://10.246.140.36/userValidate?mobile=9633691230&validation_type=mobile&id=0
http://10.246.140.36/js/script.js?v=1717763431

http://10.246.140.36/js/script.js?v=1717763433
http://10.246.140.36/js/script.js?v=1717763435
http://10.246.140.36/js/script.js?v=1717763436
http://10.246.140.36/js/script.js?v=1717763437
http://10.246.140.36/js/script.js?v=1717763438
http://10.246.140.36/js/script.js?v=1717763440
http://10.246.140.36/js/script.js?v=1717763441
http://10.246.140.36/js/script.js?v=1717763445
http://10.246.140.36/js/script.js?v=1717763452
http://10.246.140.36/aboutus
http://10.246.140.36/js/script.js?v=1717763454
http://10.246.140.36/js/script.js?v=1717763456
http://10.246.140.36/rules
http://10.246.140.36/js/script.js?v=1717763457
http://10.246.140.36/js/script.js?v=1717763458
http://10.246.140.36/js/script.js?v=1717763459
http://10.246.140.36/feedback
http://10.246.140.36/js/script.js?v=1717763460
http://10.246.140.36/js/feedback-form.js
http://10.246.140.36/js/script.js?v=1717763463
http://10.246.140.36/js/script.js?v=1717763464
http://10.246.140.36/js/script.js?v=1717763465
http://10.246.140.36/js/script.js?v=1717763466
http://10.246.140.36/js/script.js?v=1717763468
http://10.246.140.36/contactus
http://10.246.140.36/js/script.js?v=1717763469
http://10.246.140.36/js/script.js?v=1717763470
http://10.246.140.36/js/script.js?v=1717763471
http://10.246.140.36/js/script.js?v=1717763472
http://10.246.140.36/js/script.js?v=1717763474
http://10.246.140.36/js/script.js?v=1717763475
http://10.246.140.36/js/script.js?v=1717763477
http://10.246.140.36/js/script.js?v=1717763478
http://10.246.140.36/js/script.js?v=1717763480
http://10.246.140.36/js/script.js?v=1717763482
http://10.246.140.36/js/script.js?v=1717763484
http://10.246.140.36/js/script.js?v=1717763485
http://10.246.140.36/forgot-password
http://10.246.140.36/change-password
http://10.246.140.36/proposals/accepted?s=1234
http://10.246.140.36/2fa/reset
http://10.246.140.36/js/script.js?v=1717763560
http://10.246.140.36/js/script.js?v=1717763561
http://10.246.140.36/feedback
http://10.246.140.36/js/script.js?v=1717763562
http://10.246.140.36/js/script.js?v=1717763527
http://10.246.140.36/js/forgot.js
http://10.246.140.36/forgot-password/email
http://10.246.140.36/logout

http://10.246.140.36/js/script.js?v=1717763567
http://10.246.140.36/js/jquery-3.7.1.min.js
http://10.246.140.36/profile
http://10.246.140.36/vendor/bootstrap/js/bootstrap.min.js
http://10.246.140.36/js/script.js?v=1717763549
http://10.246.140.36/js/datatable.js
http://10.246.140.36/js/script.js?v=1717763534
http://10.246.140.36/js/jquery.validate.min.js
http://10.246.140.36/vendor/select2/select2.min.js
http://10.246.140.36/vendor/bootstrap/js/bootstrap-select.min.js
http://10.246.140.36/js/forge.min.js
http://10.246.140.36/js/login.js
http://10.246.140.36/js/script.js?v=1717763585
http://10.246.140.36/login
http://10.246.140.36/login
http://10.246.140.36/home
http://10.246.140.36/2fa
http://10.246.140.36/2fa

Failed Requests 14

TOC

URL	Reason
http://10.246.140.36/proposals/proceed-esign-approval-letter	Response Status '500' - Internal Server Error
http://10.246.140.36/logout	Response Status '405' - Method Not Allowed
http://10.246.140.36/vendor/bootstrap/js/popper.js	Response Status '404' - Not Found
http://10.246.140.36/icons/	Response Status '403' - Forbidden
http://10.246.140.36/icons/small/	Response Status '403' - Forbidden
http://10.246.140.36/cgi-bin/	Response Status '403' - Forbidden
http://10.246.140.36/assets/	Response Status '403' - Forbidden
http://10.246.140.36/images/	Response Status '403' - Forbidden
http://10.246.140.36/js/	Response Status '403' - Forbidden
http://10.246.140.36/img/	Response Status '403' - Forbidden
http://10.246.140.36/storage/	Response Status '403' - Forbidden
http://10.246.140.36/uploads/	Response Status '403' - Forbidden
http://10.246.140.36/cert/	Response Status '403' - Forbidden
http://10.246.140.36/css/	Response Status '403' - Forbidden