WAS Scan Report

Qualys. Consulting Edition

Delivered by ELEVATE

Scan Report

28 Feb 2021

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Sebastian Austin

Elevate Consult
1172 S. DIXIE HWY, SUITE 311
Coral Gables, Florida 33146
United States of America

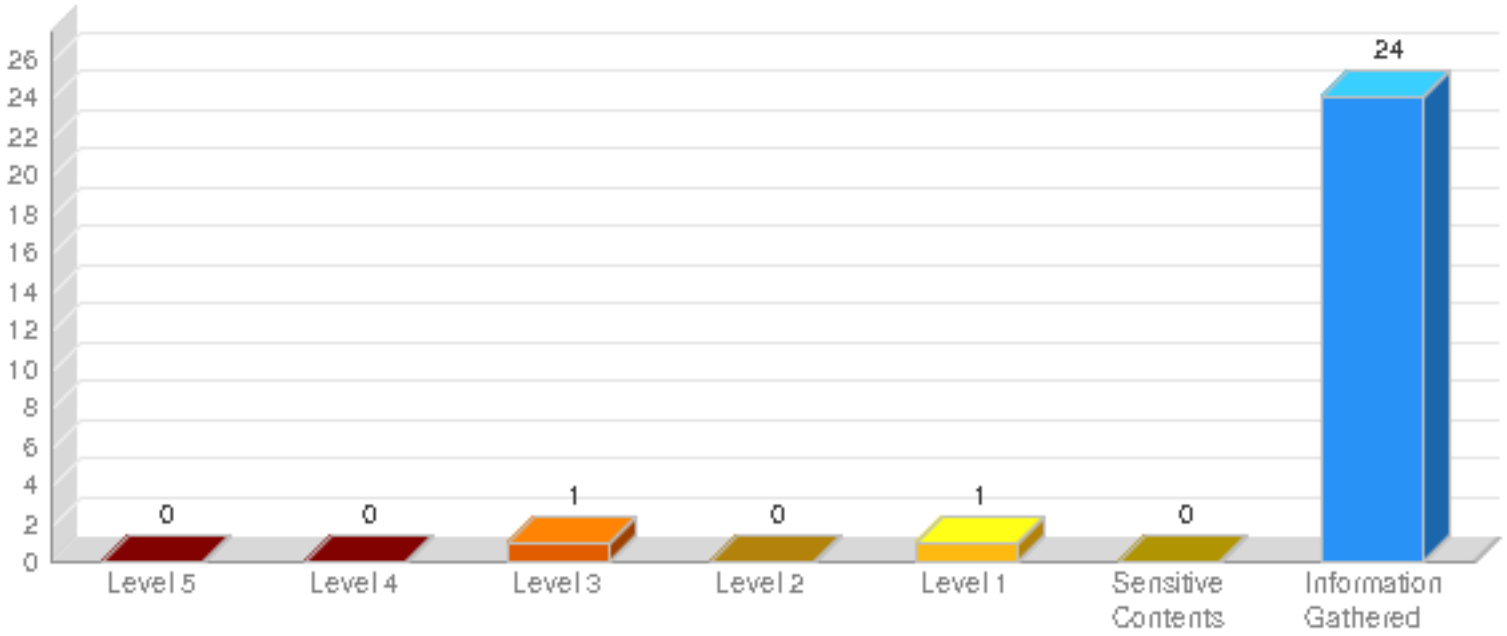
Target and Filters

Scans (1)	Acosta Insurance Group: Agent.Enterate.com AUTH Run #13
Web Applications (1)	Acosta Insurance Group: Agent.Enterate.com

Summary

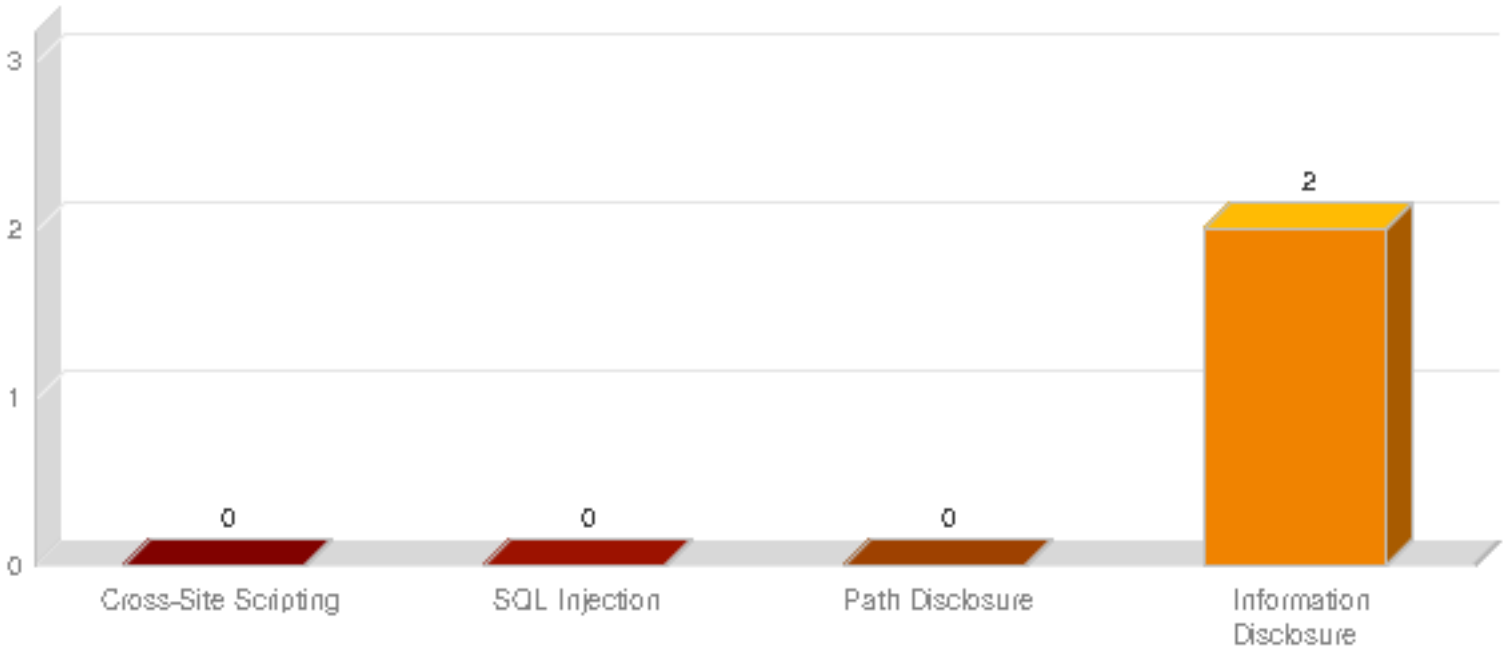
Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
MED	2	0	24

Findings by Severity

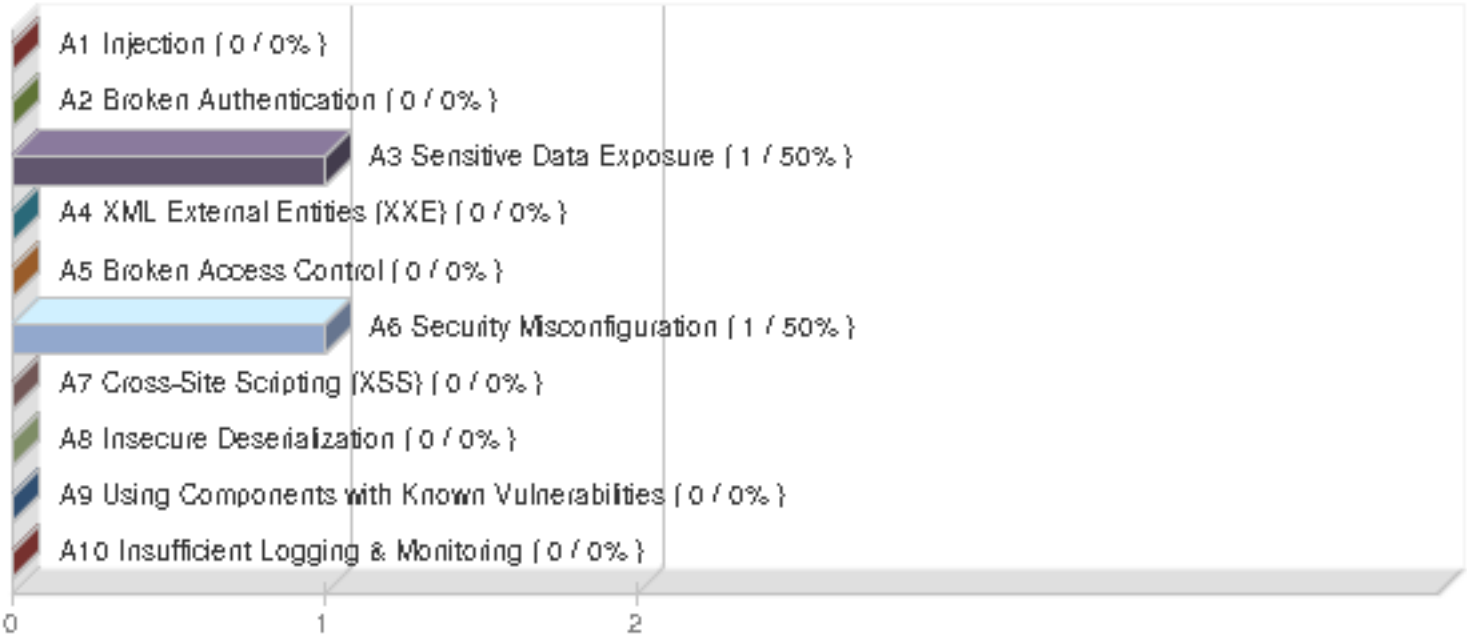


WAS Scan Report

Vulnerabilities by Group



OWASP Top 10 2017 Vulnerabilities



Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Acosta Insurance Group: Agent.Enterate.com AUTH Run #13	27 Feb 2021 23:52 GMT-0500	0	0	1	0	1	0	24

WAS Scan Report

Results(26)

Vulnerability (2)

Information Disclosure (2)

150263 Insecure Transport (1)

WAS Scan Report

150263 Insecure Transport

URL: http://agent.enterate.com/

Finding #	**9429282**(388773985)	**Severity**	Confirmed Vulnerability - Level 3
Unique #	**b9f7aaf2-7a67-4b47-9ef1-a011dfd7dab0**		
Group	Information Disclosure	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	CWE-319		
OWASP	A3 Sensitive Data Exposure		
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION		
CVSS Base	6.4	**CVSS Temporal**	5.8

Details

Threat

A link is functional over an insecure, HTTP connection. No redirection to HTTPS occurs. Note that this QID is reported for 200/OK responses as well as 4xx and 5xx responses.

Impact

Data sent over a non-HTTPS connection is unencrypted and vulnerable to network sniffing attacks that can expose sensitive or confidential information. This includes non-secure cookies and other potentially sensitive data contained in HTTP headers. Even if no sensitive data is transmitted, man-in-the-middle (MITM) attacks are possible over non-HTTPS connections. An attacker who exploits MITM can intercept and change the conversation between the client (e.g., web browser, mobile device, etc.) and the server.

More information: Why HTTPS Matters

Solution

Ensure that all links are accessible over HTTPS only. The most secure design is for the application to listen and respond only to encrypted HTTPS requests. Alternatively, if non-HTTPS requests are accepted, the server should redirect these requests to HTTPS using a 301 or 302 response.

It is also strongly recommended to use HTTP Strict Transport Security (HSTS) so that web browsers are instructed to use only HTTPS when making requests to the server. QID 150135 will be reported when links without HSTS are found.

For more information, see the Application section of OWASP's Transport Layer Protection Cheat Sheet.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

WAS Scan Report

#1 Request

GET http://agent.enterate.com/

Referer: http://agent.enterate.com/
Host: agent.enterate.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Cache-Control: no-store,no-cache,max-age=0,must-revalidate
Pragma: no-cache
Content-Type: text/html;charset=utf-8
Expires: 0
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
X-Powered-By: ASP.NET
Date: Sun, 28 Feb 2021 04:54:21 GMT
Content-Length: 8286
Set-Cookie: rsa-csrf=Z00Z002Z005B382682A77C1A3FZ00603B21FAZ00603B21FAZ00Z00Z14ZE9RZE3ZCDZEDZC4YkZ1FZ22ZDAZ99YZ20Z5BZC0ZBAZBBZ5DZ2CZE8Z876ZCAZ5CZF2Z92ZABZB7Z7C HttpOnly; domain=agent.enterate.com; path=/

http://agent.enterate.com/ response code: 200

<html><head><title>302 Moved Temporarily</title></head>
<body bgcolor="#FFFFFF">
This document you requested has moved
temporarily.
It's now at <a href="https://rsaweb.ahcadvisor.com:443/IMS-AA-IDP/virtualhost/sso/logon?RequestID=35ffd5b51e0aa8c01ae590c4d9ea9b32&MajorVersion=1&MinorVersion=2&IssueInstant=2021-02-28T04%3A54%3A21&ProviderID=urn%3Acom%3Arsasecurity%3A2004%3A10%3Asso%3Aprovider%3A0000-Global-0000%3Aims-rba-provider-webtier&IsPassive=false&AuthnCont

150081 X-Frame-Options header is not set (1)

WAS Scan Report

150081 X-Frame-Options header is not set

URL: http://agent.enterate.com/

Finding #	**9429280**(388773984)	**Severity**	Potential Vulnerability - Level 1
Unique #	**aa8fe73f-1e90-4868-aa05-532ea1ca11bb**		
Group	Information Disclosure	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	CWE-693		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		
CVSS Base	5 **CVSS Temporal** 4.1		

Details

Threat

*** NOTE: This QID has been deprecated and replaced with QID 150245 as of September 2020. This QID will be removed from WAS in the future. ***

The X-Frame-Options header is not set in the HTTP response, meaning the page can potentially be loaded into an attacker-controlled frame. This could lead to clickjacking, where an attacker adds an invisible layer on top of the legitimate page to trick users into clicking on a malicious link or taking a harmful action.

Impact

Without an X-Frame-Options response header, clickjacking may be possible. However, if the application properly uses the Content-Security-Policy "frame-ancestors" directive, then modern web browsers would stop the page from being framed and prevent clickjacking.

Solution

The X-Frame-Options allows three values: DENY, SAMEORIGIN and ALLOW-FROM. It is recommended to use DENY, which prevents all domains from framing the page or SAMEORIGIN, which allows framing only by the same site. DENY and SAMEORGIN are supported by all browsers. Using ALLOW-FROM is not recommended because not all browsers support it.

Note: To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

It is also recommended to use the Content-Security-Policy "frame-ancestors directive". For more information, see the OWASP Clickjacking Defense Cheat Sheet

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

GET http://agent.enterate.com/

Host: agent.enterate.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

The response for this request either did not have an "X-FRAME-OPTIONS" header present or was not set to DENY or SAMEORIGIN

WAS Scan Report

Information Gathered (24)

Information Gathered (1)

150078 Content of sitemap.xml (1)

WAS Scan Report

150078 Content of sitemap.xml

Finding #	**2984875**(388773981)	**Severity**	Information Gathered - Level 1
Unique #	**644d3c4d-3b5e-4d08-a43f-e4e3714a30d0**		
Group	Information Gathered	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The content of the sitemap.xml file appears in the Results section.

Impact
N/A

Solution
N/A

Results

Sitemap URI:http://agent.enterate.com/sitemap.xml

```
<html><head><title>RSA SecurID PASSCODE Request</title>


<script language="JavaScript">
<!--

function getError()
{
 return "";
}
function getUrl()
{
 return "/WebID/IISWebAgentIF.dll";
}


var need_cancel = true;
var submitDone = false;
function dopopup( location, w, h ) {
 return window.open(location, "SecurIDPopup", "screenx=16,screeny=16,left=16,top=16,height=" + h + ",width=" + w);
}
function clear_cancel() {
 need_cancel = false;
 if (submitDone) return false;
 submitDone = true;
 //var myform=document.forms[0];
 //document.cookie = "username=" + myform.username.value + ";path=/;";
 return true;
}
function check_cancel() {
 if (need_cancel) {
 dopopup("/WebID/IISWebAgentIF.dll?Cancel?sessionid=0&authntype=2", 500, 240);
 }
}

function frametop()
{
 if (!(top === self))
 {
 document.write = '';
 setTimeout(function(){document.body.innerHTML='';},1);
 window.self.onload=function(evt){document.body.innerHTML='';};
 window.top.location = wind
...(truncated)
```

WAS Scan Report

Scan Diagnostics (13)

45017 Operating System Detected (1)

45017 Operating System Detected

Finding #	**2984872**(388773978)	**Severity**	Information Gathered - Level 2
Unique #	**c0e375c1-52e4-4640-b043-20879fe350ac**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint**: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS**: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info**: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP**: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

Impact

Not applicable.

Solution

Not applicable.

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	173.230.231.244
Port	-
Result	Windows_Vista_/_Windows_2008_/_Windows_7_/_Windows_2012 TCP/IP_Fingerprint U3423:80

WAS Scan Report

150018 Connection Error Occurred During Web Application Scan (1)

150018 Connection Error Occurred During Web Application Scan

Finding #	**2984858**(388773960)	**Severity**	Information Gathered - Level 2
Unique #	**852a7611-a8f5-41b5-a388-da9ed85d335c**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following are some of the possible reasons for the timeouts or connection errors:

1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

Impact

Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

Solution

First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure blacklists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

Results

Total number of unique links that encountered timeout errors: 2
Links with highest number of timeouts:
1 http://agent.enterate.com/robots.txt
1 http://agent.enterate.com/sitemap.xml

Phase wise summary of timeout and connection errors encountered:
ePhaseShellShock : 2 0

6 DNS Host Name (1)

WAS Scan Report

6 DNS Host Name

Finding #	**2984862**(388773964)	**Severity**	Information Gathered - Level 1
Unique #	**757004d1-7a0f-4f83-96f3-4d0b18d92bb8**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	173.230.231.244
Port	-
Result	#table IP_address Host_name 173.230.231.244 web1.enterate.com

45038 Host Scan Time (1)

WAS Scan Report

45038 Host Scan Time

Finding #	**3084222**(388773970)	**Severity**	Information Gathered - Level 1
Unique #	**e1f6cf7c-472e-4c89-8d0f-3513690ac0dc**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

For host running the Qualys Windows agent this QID reports the time taken by the agent to collect the host metadata used for the most recent assessment scan.

Impact

N/A

Solution

N/A

Results

Scan duration: 898 seconds

Start time: Sun, Feb 28 2021, 04:52:13 GMT

End time: Sun, Feb 28 2021, 05:07:11 GMT

150006 Web Application Authentication Not Attempted (1)

WAS Scan Report

150006 Web Application Authentication Not Attempted

Finding #	**2984636**(388773972)	**Severity**	Information Gathered - Level 1
Unique #	**be9d2994-79ab-43de-80be-7e357fdcbf33**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Web application authentication was enabled for the scan, but it was not performed for this particular host. It was not performed because a login page was not discovered, or a login page was discovered that submits via HTTP and the scan configuration requires that credentials be submitted via HTTPS.

Impact

Vulnerabilities that require authentication may not be detected.

Solution

To allow web application authentication to this host, use an appropriate authentication record and ensure the login page is in the crawl scope. Also, if the web application does not support HTTPS, the scan configuration needs to allow transmission of credentials over plaintext HTTP connections.

Results

Application authentication was specified, but no login forms were discovered during the crawl.

150009 Links Crawled (1)

WAS Scan Report

150009 Links Crawled

Finding #	**2984873**(388773979)	**Severity**	Information Gathered - Level 1
Unique #	**9fa0ac33-4bc7-419b-9fdd-402bb5c9e9ac**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

Impact

N/A

Solution

N/A

Results

Duration of crawl phase (seconds): 176.00
Number of links: 4
(This number excludes form requests and links re-requested during authentication.)

http://agent.enterate.com/
http://agent.enterate.com/crossdomain.xml
http://agent.enterate.com/robots.txt
http://agent.enterate.com/sitemap.xml

150010 External Links Discovered (1)

WAS Scan Report

150010 External Links Discovered

Finding #	**2984869**(388773975)	**Severity**	Information Gathered - Level 1
Unique #	**a3a0a28d-133f-4046-b9ad-4925bfe94c21**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Impact
N/A

Solution
N/A

Results

Number of links: 5
https://rsaweb.ahcadvisor.com/IMS-AA-IDP/Error.jsp
https://rsaweb.ahcadvisor.com:443/IMS-AA-IDP/virtualhost/sso/logon?
RequestID=35ffd5b51e0aa8c01ae590c4d9ea9b32&MajorVersion=1&MinorVersion=2&IssueInstant=2021-02-28T04%3A54%3A21&ProviderID=urn%3Acom%3Arsasecurity%3A2004%3A10%3Asso
%3Aprovider%3A0000-Global-0000%3Aims-rba-provider-webtier&IsPassive=false&AuthnContextClassRef=urn%3Acom%3Arsasecurity%3A2004%3A08%3Aauthn%3Apolicy
%3A00000000000000000000001000f0023002%20urn%3Acom%3Arsasecurity%3A2006%3A08%3Aauthn%3Asessionlifetime
%3A00000000000000000000001000c0027099&AuthnContextComparison=exact&RelayState=https%3A%2F%2Frsaweb%2Eahcadvisor%2Ecom%3A443%2Fims-rba%2Findex%2Ejsp&rsa
%3AClientAddress=64%2E39%2E99%2E119&rsa%3AAgentID=ims%2Efd2eeea11e0aa8c0388603289e0e14bb&rsa%3ASSOFlags=0&SigAlg=http%3A%2F%2Fwww%2Ew3%2Eorg
%2F2000%2F09%2Fxmldsig%23rsa-
sha1&Signature=VdAnlbb1oaRY9y48arPOTlHmOG3PgHIU0ytXADbq4Eouun1WmrlwdlOeNLlbHy6ERCXTVNzFvSWjBLn7wqJj0f3H5%2Fny7%2FQU5fw27PLAF4o9QoIDYi4bLHsGGvhsbXsDT
%2BW%2F%2BaSY%2FBs%2BGTjTHtliMoYrNwUG5KNyWCUYZ%2BR%2F0hurS%2BLflzFNbDFMg2MCLKperHUJuwQYRic9ycEeIDQBbTe0m72slTmqerBxfuv
%2FJlFSqFMVoH2bfJ3L1UJOLQkPB%2F3e7ICR%2FT5%2B5eC4rsuw%3D%3D
https://rsaweb.ahcadvisor.com/IMS-AA-IDP/virtualhost/sso/logon?
RequestID=35ffd5b51e0aa8c01ae590c4d9ea9b32&MajorVersion=1&MinorVersion=2&IssueInstant=2021-02-28T04%3A54%3A21&ProviderID=urn%3Acom%3Arsasecurity%3A2004%3A10%3Asso
%3Aprovider%3A0000-Global-0000%3Aims-rba-provider-webtier&IsPassive=false&AuthnContextClassRef=urn%3Acom%3Arsasecurity%3A2004%3A08%3Aauthn%3Apolicy
%3A00000000000000000000001000f0023002%20urn%3Acom%3Arsasecurity%3A2006%3A08%3Aauthn%3Asessionlifetime
%3A00000000000000000000001000c0027099&AuthnContextComparison=exact&RelayState=https%3A%2F%2Frsaweb.ahcadvisor.com%3A443%2Fims-rba%2Findex.jsp&rsa
%3AClientAddress=64.39.99.119&rsa%3AAgentID=ims.fd2eeea11e0aa8c0388603289e0e14bb&rsa%3ASSOFlags=0&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
sha1&Signature=VdAnlbb1oaRY9y48arPOTlHmOG3PgHIU0ytXADbq4Eouun1WmrlwdlOeNLlbHy6ERCXTVNzFvSWjBLn7wqJj0f3H5%2Fny7%2FQU5fw27PLAF4o9QoIDYi4bLHsGGvhsbXsDT
%2BW%2F%2BaSY%2FBs%2BGTjTHtliMoYrNwUG5KNyWCUYZ%2BR%2F0hurS%2BLflzFNbDFMg2MCLKperHUJuwQYRic9ycEeIDQBbTe0m72slTmqerBxfuv
%2FJlFSqFMVoH2bfJ3L1UJOLQkPB%2F3e7ICR%2FT5%2B5eC4rsuw%3D%3D
https://rsaweb.ahcadvisor.com/IMS-AA-IDP/virtualhost/sso/logon?
RequestID=b17586821e0aa8c07c119b1656f7d288&MajorVersion=1&MinorVersion=2&IssueInstant=2021-02-28T04%3A54%3A19&ProviderID=urn%3Acom%3Arsasecurity
%3A2004%3A10%3Asso%3Aprovider%3A0000-Global-0000%3Aims-rba-provider-webtier&IsPassive=false&AuthnContextClassRef=urn%3Acom%3Arsasecurity%3A2004%3A08%3Aauthn
%3Apolicy%3A00000000000000000000001000f0023002%20urn%3Acom%3Arsasecurity%3A2006%3A08%3Aauthn%3Asessionlifetime
%3A00000000000000000000001000c0027099&AuthnContextComparison=exact&RelayState=https%3A%2F%2Frsaweb.ahcadvisor.com%3A443%2Fims-rba%2Findex.jsp&rsa
%3AClientAddress=64.39.99.119&rsa%3AAgentID=ims.fd2eeea11e0aa8c0388603289e0e14bb&rsa%3ASSOFlags=0&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
sha1&Signature=MCDkGf%2FjejG7WxE3RyyMjxVOjfOK2BW3upyJ4aM79BCxXbyY4w9nO%2BhMntZa9Wpa%2BSr%2BbhoJV
%2BTa6MuXeRI9ygDC9qPrgvd2K8bJf1EWnFgHDlYKGkYFVV0rXjNwKawgtQlNyInFlufHa8bFafVajf9yudLn2iN8lJa2MBqHcZRCVJdbxjVrhh6qmLNuU9slInWbCFkpTymb6KTaIWezQtw91BckJ
%2Bh1kkYdmK3Emu1%2FkWYjmaSl%2Bd2zgUbWe8orx3cY8HrDlXKCRIE3e2z7Z%2Fhvm%2BAv3dUvleeeWQTjBayMBLHc%2FfMTzUmE4CGVMM7t0EVLu8Q%3D%3D
https://rsaweb.ahcadvisor.com/ims-rba/

150021 Scan Diagnostics (1)

WAS Scan Report

150021 Scan Diagnostics

Finding #	**2984863**(388773965)	**Severity**	Information Gathered - Level 1
Unique #	**ef6ee77b-a03d-4d93-b0c9-a35607bbbdd3**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution

No action is required.

Results

Loaded 0 blacklist entries.
Loaded 0 whitelist entries.
Target web application page http://agent.enterate.com/ fetched. Status code:200, Content-Type:text/html, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 10 minutes (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 4 seconds. Completed 70 requests of 70 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found. Aborting the CMS Detection phaseCMSDetection: 1 vulnsigs tests, completed 48 requests, 5 seconds. Completed 48 requests of 48 estimated requests (100%). All tests completed.
Collected 4 links overall in 0 hours 2 minutes duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 3) + files:(0 x 3) + directories:(9 x 1) + paths:(0 x 4) = total (9)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 4 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.
Batch #0 WS enumeration: estimated time < 1 minute (11 tests, 4 inputs)
WS enumeration: 11 vulnsigs tests, completed 14 requests, 1 seconds. Completed 14 requests of 44 estimated requests (31.8182%). All tests completed.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (70 tests, 0 inputs)
Batch #1 URI parameter manipulation (no auth): 70 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 0 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 0 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 0 inputs)
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 WebCgiOob: estimated time < 1 minute (6 tests, 1 inputs)
Batch #4 WebCgiOob: 6 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 36 estimated requests (0%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 1 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 8 requests, 16 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (38 tests, 0 inputs)
Batch #4 HTTP call manipulation: 38 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (3 tests, 0 inputs)
Batch #4 Open Redirect analysis: 3 vulnsigs tests, completed 0 requests, 3 seconds. No tests to execute.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 4 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 4 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (46 tests, 1 inputs)
Batch #4 Cookie manipulation: 46 vulnsigs tests, completed 68 requests, 4 seconds. Completed 68 requests of 68 estimated requests (100%). XSS optimization removed 116 links. All tests completed.
Batch #4 Header manipulation: estimated time < 1 minute (46 tests, 4 inputs)
Batch #4 Header manipulation: 46 vulnsigs tests, completed 236 requests, 11 seconds. Completed 236 requests of 504 estimated requests (46.8254%). XSS optimization removed 116 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 4 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 4 requests, 300 seconds. Completed 4 requests of 4 estimated requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 httpoxy detector: estimated time < 1 minute (1 tests, 4 inputs)
Batch #4 httpoxy detector: 1 vulnsigs tests, completed 4 requests, 1 seconds. Completed 4 requests of 4 estimated requests (100%). All tests completed.
Batch #4 httpoxy detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 httpoxy detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Struts timebased detector: estimated time < 1 minute (1 tests, 4 inputs)
Batch #4 Struts timebased detector: 1 vulnsigs tests, completed 4 requests, 0 seconds. Completed 4 requests of 4 estimated requests (100%). All tests completed.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 3) + files:(0 x 3) + directories:(4 x 1) + paths:(11 x 4) = total (48)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 4 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 47 requests, 2 seconds. Completed 47 requests of 48 estimated requests (97.9167%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 3) + files:(0 x 3) + directories:(1 x 1) + paths:(0 x 4) = total (1)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 4 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 3) + files:(0 x 3) + directories:(16 x 1) + paths:(0 x 4) = total (16)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 4 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 32 requests, 360 seconds. Completed 32 requests of 16 estimated requests (200%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 3) + files:(18 x 3) + directories:(124 x 1) + paths:(18 x 4) = total (262)
Batch #5 Path manipulation: estimated time < 1 minute (164 tests, 4 inputs)
Batch #5 Path manipulation: 164 vulnsigs tests, completed 222 requests, 8 seconds. Completed 222 requests of 262 estimated requests (84.7328%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 minute (54 tests, 1 inputs)
Batch #5 WebCgiGeneric: 54 vulnsigs tests, completed 56 requests, 4 seconds. Completed 56 requests of 360 estimated requests (15.5556%). All tests completed.
Total requests made: 865
Average server response time: 0.16 seconds

150028 Cookies Collected (1)

150028 Cookies Collected

Finding #	**2984865**(388773969)	**Severity**	Information Gathered - Level 1
Unique #	**29335cdc-8342-43c6-9bcf-85dd705ff669**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The cookies listed in the Results section were set by the web application during the crawl phase.

Impact
Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

Solution
Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

Results

Total cookies: 3
rsa-
csrf=Z00Z002Z005B382682A77C1A3FZ00603B21FAZ00603B21FAZ00Z00Z14ZE9RZE3ZCDZEDZC4YkZ1FZ22ZDAZ99YZ20Z5BZC0ZBAZBBZ5DZ2CZE8Z876ZCAZ5CZF2Z92ZABZB7Z7CV
HttpOnly; path=/ First set at URL: http://agent.enterate.com/
ims-rba-jsessionid=r8nm_L00z9giwc5ogXNEDdnF1LBK1p93eNB9L4aJwOb_EHVf4c0j!1875276253; secure; HttpOnly; path=/ims-rba First set at URL: https://rsaweb.ahcadvisor.com/ims-rba/
ims-aa-idp-jsessionid=08zm_L1jYxesd8cCgy8Pvr5h0btxVHmTN57B8Wn5GS4yCq9hcw7K!1875276253; secure; HttpOnly; path=/ First set at URL: https://rsaweb.ahcadvisor.com/IMS-AA-IDP/
virtualhost/sso/logon?RequestID=b17586821e0aa8c07c119b1656f7d288&MajorVersion=1&MinorVersion=2&IssueInstant=2021-02-28T04%3A54%3A19&ProviderID=urn%3Acom%3Arsasecurity
%3A2004%3A10%3Asso%3Aprovider%3A0000-Global-0000%3Aims-rba-provider-webtier&IsPassive=false&AuthnContextClassRef=urn%3Acom%3Arsasecurity%3A2004%3A08%3Aauthn
%3Apolicy%3A0000000000000000000001000f0023002 urn%3Acom%3Arsasecurity%3A2006%3A08%3Aauthn%3Asessionlifetime
%3A0000000000000000000001000c0027099&AuthnContextComparison=exact&RelayState=https%3A%2F%2Frsaweb.ahcadvisor.com%3A443%2Fims-rba%2Findex.jsp&rsa
%3AClientAddress=64.39.99.119&rsa%3AAgentID=ims.fd2eeea11e0aa8c0388603289e0e14bb&rsa%3ASSOFlags=0&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
sha1&Signature=MCDkGf%2FjejG7WxE3RyyMjxVOjfOK2BW3upyJ4aM79BCxXbyY4w9nO%2BhMntZa9Wpa%2BSr%2BbhoJV
%2BTa6MuXeRI9ygDC9qPrgvd2K8bJf1EWnFgHDlYKGkYFVV0rXjNwKawgtQlNyInFlufHa8bFafVajf9yudLn2iN8lJa2MBqHcZRCVJdbxjVrhh6qmLNuU9slInWbCFkpTymb6KTaIWezQtw91BckJ
%2Bh1kkYdmK3Emu1%2FkWYjmaSl%2Bd2zgUbWe8orx3cY8HrDlXKCRIE3e2z7Z%2Fhvm%2BAv3dUvleeeWQTjBayMBLHc%2FfMTzUmE4CGVMM7t0EVLu8Q%3D%3D

150041 Links Rejected (1)

WAS Scan Report

150041 Links Rejected

Finding #	**2984874**(388773980)	**Severity**	Information Gathered - Level 1
Unique #	**3665f0ac-51a7-488c-92bd-b27bb2c779a9**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This has an informative nature. The links listed below were not crawled by the Web application scanning engine because they were intentionally prohibited by a blacklist or whitelist configuration setting. The list is provided to verify that links have been correctly blocked by blacklist and whitelist filters.

Impact

Links listed here were neither crawled or tested by the Web application scanning engine, and that should be in sync with the intended behavior.

Solution

No action is required.

Results

http://agent.enterate.com/WebID/IISWebAgentIF.dll?Cancel%3Fsessionid=0&authntype=2
http://agent.enterate.com/WebID/IISWebAgentIF.dll?GetFile%3Ffile=useridandpasscodeplugin
http://agent.enterate.com/WebID/IISWebAgentIF.dll?GetFile%3Ffile=useridandpasscodemanual

150077 Content of robots.txt (1)

WAS Scan Report

150077 Content of robots.txt

Finding #	**2984877**(388773983)	**Severity**	Information Gathered - Level 1
Unique #	**faa5c3e6-49eb-43ea-8129-7ebfb5152a57**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The content of the robots.txt file appears in the Results section.

Impact
N/A

Solution
N/A

Results

Robots.txt URI:http://agent.enterate.com/robots.txt

```
<html><head><title>RSA SecurID PASSCODE Request</title>


<script language="JavaScript">
<!--

function getError()
{
 return "";
}
function getUrl()
{
 return "/WebID/IISWebAgentIF.dll";
}


var need_cancel = true;
var submitDone = false;
function dopopup( location, w, h ) {
 return window.open(location, "SecurIDPopup", "screenx=16,screeny=16,left=16,top=16,height=" + h + ",width=" + w);
}
function clear_cancel() {
 need_cancel = false;
 if (submitDone) return false;
 submitDone = true;
 //var myform=document.forms[0];
 //document.cookie = "username=" + myform.username.value + ";path=/;";
 return true;
}
function check_cancel() {
 if (need_cancel) {
 dopopup("/WebID/IISWebAgentIF.dll?Cancel?sessionid=0&authntype=2", 500, 240);
 }
}

function frametop()
{
 if (!(top === self))
 {
 document.write = '';
 setTimeout(function(){document.body.innerHTML='';},1);
 window.self.onload=function(evt){document.body.innerHTML='';};
 window.top.location = wind
...(truncated)
```

150106 Content of crossdomain.xml (1)

WAS Scan Report

150106 Content of crossdomain.xml

Finding #	**2984870**(388773976)	**Severity**	Information Gathered - Level 1
Unique #	**e79537a2-f506-4e0c-a467-d720309983d7**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The content of the crossdomain.xml file appears in the Results section.

Impact
N/A

Solution
N/A

Results

```
crossdomain.xml found is not valid
Content-Type:text/html
Showing only a part of the response
<html><head><title>RSA SecurID PASSCODE Request</title>


<script language="JavaScript">
<!--

function getError()
{
 return "";
}
function getUrl()
{
 return "/WebID/IISWebAgentIF.dll";
}


var need_cancel = true;
var submitDone = false;
function dopopup( location, w, h ) {
 return window.open(location, "SecurIDPopup", "screenx=16,screeny=16,left=16,top=16,height=" + h + ",width=" + w);
}
function clear_cancel() {
 need_cancel = false;
 if (submitDone) return false;
 submitD
```

150152 Forms Crawled (1)

WAS Scan Report

150152 Forms Crawled

Finding #	**2984864**(388773968)	**Severity**	Information Gathered - Level 1
Unique #	**69cb2a51-25b4-40ff-9b04-875d3481bb80**		
Group	Scan Diagnostics	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

Impact

N/A

Solution

N/A

Results

Total internal forms seen (this count includes duplicate forms): 0

Crawled forms (Total: 0)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115

Security Weaknesses (10)

150086 Server accepts unnecessarily large POST request body (1)

WAS Scan Report

150086 Server accepts unnecessarily large POST request body

Finding #	**2984861**(388773963)	**Severity**	Information Gathered - Level 3
Unique #	**878ebb7e-1470-4269-9c82-7243d07ac4d8**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The scanner successfully sent a POST request with content type of application/x-www-form-urlencoded and 65536 bytes length random text data. Accepting request bodies with unnecessarily large size could help attacker to use less connections to achieve Layer 7 DDoS of web server. More information can be found at the here

Impact

Potentially could result in a successful application-layer DDoS attack.

Solution

Limit the size of the request body to each form's requirements. For example, a search form with 256-char search field should not accept more than 1KB value. Server-specific details can be found here.

Results

Server responded 200 to unnecessarily large random request body(over 64 KB) for URL http://agent.enterate.com/, significantly increasing attacker's chances to prolong slow HTTP POST attack.

150210 Information Disclosure via Response Header (1)

WAS Scan Report

150210 Information Disclosure via Response Header

Finding #	**2984859**(388773961)	**Severity**	Information Gathered - Level 3
Unique #	**c05f0bdc-495c-4437-9ab7-4337213d356f**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

HTTP response headers like 'Server', 'X-Powered-By', 'X-AspNetVersion', 'X-AspNetMvcVersion' could disclose information about the platform and technologies used by the website. The HTTP response include one or more such headers.

Impact

The headers can potentially be used by attackers for fingerprinting and launching attacks specific to the technologies and versions used by the web application. These response headers are not necessary for production sites and should be disabled.

Solution

Disable such response headers, remove them from the response, or make sure that the header value does not contain information which could be used to fingerprint the server-side components of the web application.

Results

One or more response headers disclosing information about the application platform were present on the following pages:
(Only first 50 such pages are reported)

GET http://agent.enterate.com/ response code: 200
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET

150202 Missing header: X-Content-Type-Options (1)

WAS Scan Report

150202 Missing header: X-Content-Type-Options

Finding #	**2984871**(388773977)	**Severity**	Information Gathered - Level 2
Unique #	**b06d8dc6-e6c8-4757-8b9e-4c788ca3c4c4**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Content-Type-Options response header is not present. WAS reports missing X-Content-Type-Options header on each crawled link for both static and dynamic responses. The scanner performs the check not only on 200 responses but 4xx and 5xx responses as well. It's also possible the QID will be reported on directory-level links.

Impact

All web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. If X-Content-Type-Options header is not present, browsers can potentially be tricked into treating non-HTML response as HTML. An attacker can then potentially leverage the functionality to perform a cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack.

Solution

It is recommended to disable browser content sniffing by adding the X-Content-Type-Options header to the HTTP response with a value of 'nosniff'. Also, ensure that the 'Content-Type' header is set correctly on responses.

Results

X-Content-Type-Options: Header missing
Response headers on link: GET http://agent.enterate.com/ response code: 200
Cache-Control: no-store,no-cache,max-age=0,must-revalidate
Pragma: no-cache
Content-Type: text/html;charset=utf-8
Expires: 0
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
X-Powered-By: ASP.NET
Date: Sun, 28 Feb 2021 04:54:21 GMT
Content-Length: 8286
Set-Cookie: rsa-
csrf=Z00Z002Z005B382682A77C1A3FZ00603B21FAZ00603B21FAZ00Z00Z14ZE9RZE3ZCDZEDZC4YkZ1FZ22ZDAZ99YZ20Z5BZC0ZBAZBBZ5DZ2CZE8Z876ZCAZ5CZF2Z92ZABZB7Z7CV
HttpOnly; domain=agent.enterate.com; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET http://agent.enterate.com/ response code: 200

150206 Content-Security-Policy Not Implemented (1)

WAS Scan Report

150206 Content-Security-Policy Not Implemented

Finding #	**2984876**(388773982)	**Severity**	Information Gathered - Level 2
Unique #	**625e2a20-acb1-450b-8383-1298a9b52d08**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

Results

Content-Security-Policy: Header missing
Response headers on link: GET http://agent.enterate.com/ response code: 200
Cache-Control: no-store,no-cache,max-age=0,must-revalidate
Pragma: no-cache
Content-Type: text/html;charset=utf-8
Expires: 0
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
X-Powered-By: ASP.NET
Date: Sun, 28 Feb 2021 04:54:21 GMT
Content-Length: 8286
Set-Cookie: rsa-csrf=Z00Z002Z005B382682A77C1A3FZ00603B21FAZ00603B21FAZ00Z00Z14ZE9RZE3ZCDZEDZC4YkZ1FZ22ZDAZ99YZ20Z5BZC0ZBAZBBZ5DZ2CZE8Z876ZCAZ5CZF2Z92ZABZB7Z7CV
HttpOnly; domain=agent.enterate.com; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET http://agent.enterate.com/ response code: 200

150208 Missing header: Referrer-Policy (1)

WAS Scan Report

150208 Missing header: Referrer-Policy

Finding #	**2984860**(388773962)	**Severity**	Information Gathered - Level 2
Unique #	**e833d879-c566-4d0a-b8d0-b162135609c1**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Referrer Policy is specified for the link. WAS checks for the missing Referrer Policy on all static and dynamic pages. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found , WAS checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

Impact

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

Solution

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Results

Referrer-Policy: Header missing
Response headers on link: GET http://agent.enterate.com/ response code: 200
Cache-Control: no-store,no-cache,max-age=0,must-revalidate
Pragma: no-cache
Content-Type: text/html;charset=utf-8
Expires: 0
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
X-Powered-By: ASP.NET
Date: Sun, 28 Feb 2021 04:54:21 GMT
Content-Length: 8286
Set-Cookie: rsa-csrf=Z00Z002Z005B382682A77C1A3FZ00603B21FAZ00603B21FAZ00Z00Z14ZE9RZE3ZCDZEDZC4YkZ1FZ22ZDAZ99YZ20Z5BZC0ZBAZBBZ5DZ2CZE8Z876ZCAZ5CZF2Z92ZABZB7Z7CV
HttpOnly; domain=agent.enterate.com; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET http://agent.enterate.com/ response code: 200

150262 Missing header: Feature-Policy (1)

WAS Scan Report

150262 Missing header: Feature-Policy

Finding #	**2984867**(388773973)	**Severity**	Information Gathered - Level 2
Unique #	**5c829354-4b7c-4e10-91ae-40f3bc014042**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Feature-Policy response header is not present.

Impact

Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.

These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.

Solution

It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.

References:
- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Results

Feature-Policy: Header missing
Response headers on link: GET http://agent.enterate.com/ response code: 200
Cache-Control: no-store,no-cache,max-age=0,must-revalidate
Pragma: no-cache
Content-Type: text/html;charset=utf-8
Expires: 0
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
X-Powered-By: ASP.NET
Date: Sun, 28 Feb 2021 04:54:21 GMT
Content-Length: 8286
Set-Cookie: rsa-csrf=Z00Z002Z005B382682A77C1A3FZ00603B21FAZ00603B21FAZ00Z00Z14ZE9RZE3ZCDZEDZC4YkZ1FZ22ZDAZ99YZ20Z5BZC0ZBAZBBZ5DZ2CZE8Z876ZCAZ5CZF2Z92ZABZB7Z7CV
HttpOnly; domain=agent.enterate.com; path=/

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET http://agent.enterate.com/ response code: 200

150099 Cookies Issued Without User Consent (1)

WAS Scan Report

150099 Cookies Issued Without User Consent

Finding #	**2984866**(388773971)	**Severity**	Information Gathered - Level 1
Unique #	**073e124d-951d-4d6d-b3bd-d0d9c1b091f9**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were issued from the web application during the crawl without accepting any opt-in dialogs.

Impact

Cookies may be set without user explicitly agreeing to accept them.

Solution

Review the application to ensure that all cookies listed are supposed to be issued without user opt-in. If the EU Cookie law is applicable for this web application, ensure these cookies require user opt-in or have been classified as exempt by your organization.

Results

Total cookies: 1
rsa-csrf=Z00Z002Z00C2BFB7CCDF749C40Z00603B2385Z00603B2385Z00Z00Z87ZE1ZFFdZ1AZ86ZB0ZAEZ0BZ10kZE3Z03Z94ZC9VlZA6Z27Z99wZA7ZE9ZA1Z7CZD9ZC0Z95ZF1ZEEZD4ZCD; HttpOnly; path=/ First set at URL: http://agent.enterate.com/

150101 Third-party Cookies Collected (1)

WAS Scan Report

150101 Third-party Cookies Collected

Finding #	**2984868**(388773974)	**Severity**	Information Gathered - Level 1
Unique #	**4177ca2e-3622-4689-a6b6-587797716049**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were received from third-party web application(s) during the crawl phase.

Impact

Cookies may contain sensitive information about the user. Cookies sent via HTTP may be sniffed.

Solution

Review cookie values to ensure that sensitive information such as passwords are not present within them.

Results

Total cookies: 2
ims-rba-jsessionid=r8nm_L00z9giwc5ogXNEDdnF1LBK1p93eNB9L4aJwOb_EHVf4c0j!1875276253; secure; HttpOnly; path=/ims-rba First set at URL: https://rsaweb.ahcadvisor.com/ims-rba/
ims-aa-idp-jsessionid=08zm_L1jYxesd8cCgy8Pvr5h0btxVHmTN57B8Wn5GS4yCq9hcw7K!1875276253; secure; HttpOnly; path=/ First set at URL: https://rsaweb.ahcadvisor.com/IMS-AA-IDP/
virtualhost/sso/logon?RequestID=b17586821e0aa8c07c119b1656f7d288&MajorVersion=1&MinorVersion=2&IssueInstant=2021-02-28T04%3A54%3A19&ProviderID=urn%3Acom%3Arsasecurity
%3A2004%3A10%3Asso%3Aprovider%3A0000-Global-0000%3Aims-rba-provider-webtier&IsPassive=false&AuthnContextClassRef=urn%3Acom%3Arsasecurity%3A2004%3A08%3Aauthn
%3Apolicy%3A00000000000000000000001000f0023002 urn%3Acom%3Arsasecurity%3A2006%3A08%3Aauthn%3Asessionlifetime
%3A00000000000000000000001000c0027099&AuthnContextComparison=exact&RelayState=https%3A%2F%2Frsaweb.ahcadvisor.com%3A443%2Fims-rba%2Findex.jsp&rsa
%3AClientAddress=64.39.99.119&rsa%3AAgentID=ims.fd2eeea11e0aa8c0388603289e0e14bb&rsa%3ASSOFlags=0&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-
sha1&Signature=MCDkGf%2FjejG7WxE3RyyMjxVOjfOK2BW3upyJ4aM79BCxXbyY4w9nO%2BhMntZa9Wpa%2BSr%2BbhoJV
%2BTa6MuXeRI9ygDC9qPrgvd2K8bJf1EWnFgHDlYKGkYFVV0rXjNwKawgtQlNyInFlufHa8bFafVajf9yudLn2iN8lJa2MBqHcZRCVJdbxjVrhh6qmLNuU9slInWbCFkpTymb6KTaIWezQtw91BckJ
%2Bh1kkYdmK3Emu1%2FkWYjmaSl%2Bd2zgUbWe8orx3cY8HrDlXKCRIE3e2z7Z%2Fhvm%2BAv3dUvleeeWQTjBayMBLHc%2FfMTzUmE4CGVMM7t0EVLu8Q%3D%3D

150245 Missing header: X-Frame-Options (1)

WAS Scan Report

150245 Missing header: X-Frame-Options

Finding #	**3659682**(388773966)	**Severity**	Information Gathered - Level 1
Unique #	**0127f0c3-d41c-41d7-9a00-e2244c9300a2**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	CWE-693		
OWASP	A6 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Frame-Options header is not set in the HTTP response, meaning the page can potentially be loaded into an attacker-controlled frame. This could lead to clickjacking, where an attacker adds an invisible layer on top of the legitimate page to trick users into clicking on a malicious link or taking a harmful action.

Impact

Without an X-Frame-Options response header, clickjacking may be possible. However, if the application properly uses the Content-Security-Policy "frame-ancestors" directive, then modern web browsers would stop the page from being framed and prevent clickjacking.

Solution

The X-Frame-Options allows three values: DENY, SAMEORIGIN and ALLOW-FROM. It is recommended to use DENY, which prevents all domains from framing the page or SAMEORIGIN, which allows framing only by the same site. DENY and SAMEORGIN are supported by all browsers. Using ALLOW-FROM is not recommended because not all browsers support it.

Note: To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

Results

X-Frame-Options header is missing or not set to DENY or SAMEORIGIN for the following pages:
(Only first 10 such pages are reported)

GET http://agent.enterate.com/
Response code: 200
Response headers:
Cache-Control: no-store,no-cache,max-age=0,must-revalidate
Pragma: no-cache
Content-Type: text/html;charset=utf-8
Expires: 0
Server: Microsoft-IIS/8.5
X-Xss-Protection: 1; mode=block
X-Powered-By: ASP.NET
Date: Sun, 28 Feb 2021 04:54:21 GMT
Content-Length: 8286
Set-Cookie: rsa-csrf=Z00Z002Z005B382682A77C1A3FZ00603B21FAZ00603B21FAZ00Z00Z14ZE9RZE3ZCDZEDZC4YkZ1FZ22ZDAZ99YZ20Z5BZC0ZBAZBBZ5DZ2CZE8Z876ZCAZ5CZF2Z92ZABZB7Z7CV
HttpOnly; domain=agent.enterate.com; path=/

150277 Cookie without SameSite attribute (1)

WAS Scan Report

150277 Cookie without SameSite attribute

Finding #	**3178573**(388773967)	**Severity**	Information Gathered - Level 1
Unique #	**654a0d03-ebbf-4329-bc39-a1e8b28ca63f**		
Group	Security Weaknesses	**Detection Date**	27 Feb 2021 23:52 GMT-0500
CWE	-		
OWASP	A6 Security Misconfiguration		
WASC	-		

Details

Threat
The cookies listed in the Results section are missing the SameSite attribute.

Impact
The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

Solution
Consider adding the SameSite attribute to the cookie(s) listed.

More information:
DZone article
OWASP CSRF Prevention Cheat Sheet

Results

Total cookies: 1
rsa-
csrf=Z00Z002Z005B382682A77C1A3FZ00603B21FAZ00603B21FAZ00Z00Z14ZE9RZE3ZCDZEDZC4YkZ1FZ22ZDAZ99YZ20Z5BZC0ZBAZBBZ5DZ2CZE8Z876ZCAZ5CZF2Z92ZABZB7Z7CV
path=/; domain=agent.enterate.com; httponly | First set at URL: http://agent.enterate.com/

WAS Scan Report

Appendix

Scan Details

Acosta Insurance Group: Agent.Enterate.com AUTH Run #13

Reference	was/1614487801619.30839033
Date	27 Feb 2021 23:52 GMT-0500
Mode	Scheduled
Type	Vulnerability
Authentication	Acosta_Agent_login
Scanner Appliance	External (IP: 64.39.99.119, Scanner: 12.2.62-1, WAS: 8.6.21-1, Signatures: 2.5.118-2)
Profile	Initial WAS Options
DNS Override	-
Duration	00:14:58
Status	Finished
Authentication Status	Not used

Option Profile Details

Form Submission	BOTH
Form Crawl Scope	Do not include form action URI in uniqueness calculation
Maximum links to test in scope	300
User Agent	-
Request Parameter Set	Initial Parameters
Document Type	Ignore common binary files
Enhanced Crawling	Disabled
SmartScan	Disabled
Timeout Error Threshold	100
Unexpected Error Threshold	300
Performance Settings	Pre-defined
Bruteforce Option	Minimal
Detection Scope	Core
Include additional XSS payloads	No
Credit Card Numbers Search	Off
Social Security Numbers (US) Search	Off

Web Application Details: Acosta Insurance Group: Agent.Enterate.com

Name	Acosta Insurance Group: Agent.Enterate.com
ID	177024661
URL	http://Agent.enterate.com
Owner	Orlando Santa Cruz (eevat2rs)
Scope	Limit to URL hostname
Tags	-
Custom Attributes	-

Severity Levels

Confirmed Vulnerabilities

WAS Scan Report

Vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

Minimal — **Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.**

Medium — **Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.**

Serious — **Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.**

Critical — **Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.**

Urgent — **Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.**

Potential Vulnerabilities

Potential Vulnerabilities indicate that the scanner observed a weakness or error that is commonly used to attack a web application, and the scanner was unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following-up with manual analysis. For example, the exploitability of a QID may be influenced by characteristics that the scanner cannot confirm, such as the web application's network architecture, or the test to confirm exploitability requires more intrusive testing than the scanner is designed to conduct.

Minimal — **Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.**

Medium — **Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.**

Serious — **Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.**

Critical — **Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.**

Urgent — **Presence of this vulnerability might enable intruders to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. For example in this scenario, the web application users can potentially be targeted if the application is exploited.**

Sensitive Content

Sensitive content may be detected based on known patterns (credit card numbers, social security numbers) or custom patterns (strings, regular expressions), depending on the option profile used. Intruders may gain access to sensitive content that could result in misuse or other exploits.

Minimal — **Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.**

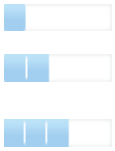
Medium — **Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.**

Serious — **Sensitive content was found in the web server response - a valid social security number or credit card information. This infomation disclosure could result in a confidentiality breach, and it gives intruders access to valid sensitive content that could be misused.**

Information Gathered

WAS Scan Report

Information Gathered issues (QIDs) include visible information about the web application's platform, code, or architecture. It may also include information about users of the web application.



Minimal	**Intruders may be able to retrieve sensitive information related to the web application platform.**
Medium	**Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.**
Serious	**Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.**