WAS Scan Report

Scan Report

11 Aug 2017

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

Alejandro López López
temex_al

Telmex Colombia
Carrera 11a #94-76 Of. 205
Bogotá, None 11001000
Colombia

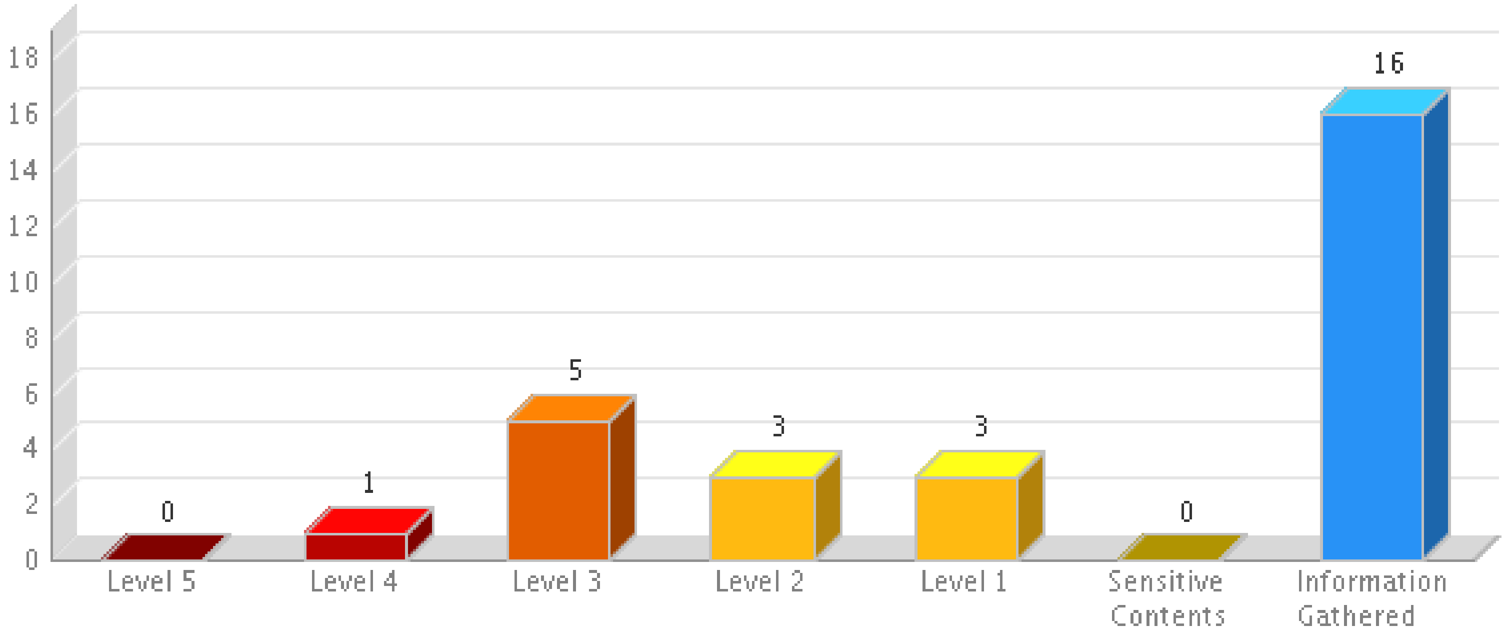
Target and Filters

Scans (1)	**Relaunch Relaunch Relaunch Relaunch Relaunch WAS_DIME2**
Web Applications (1)	**WAS_DIME**

Summary

Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
HIGH	12	0	16

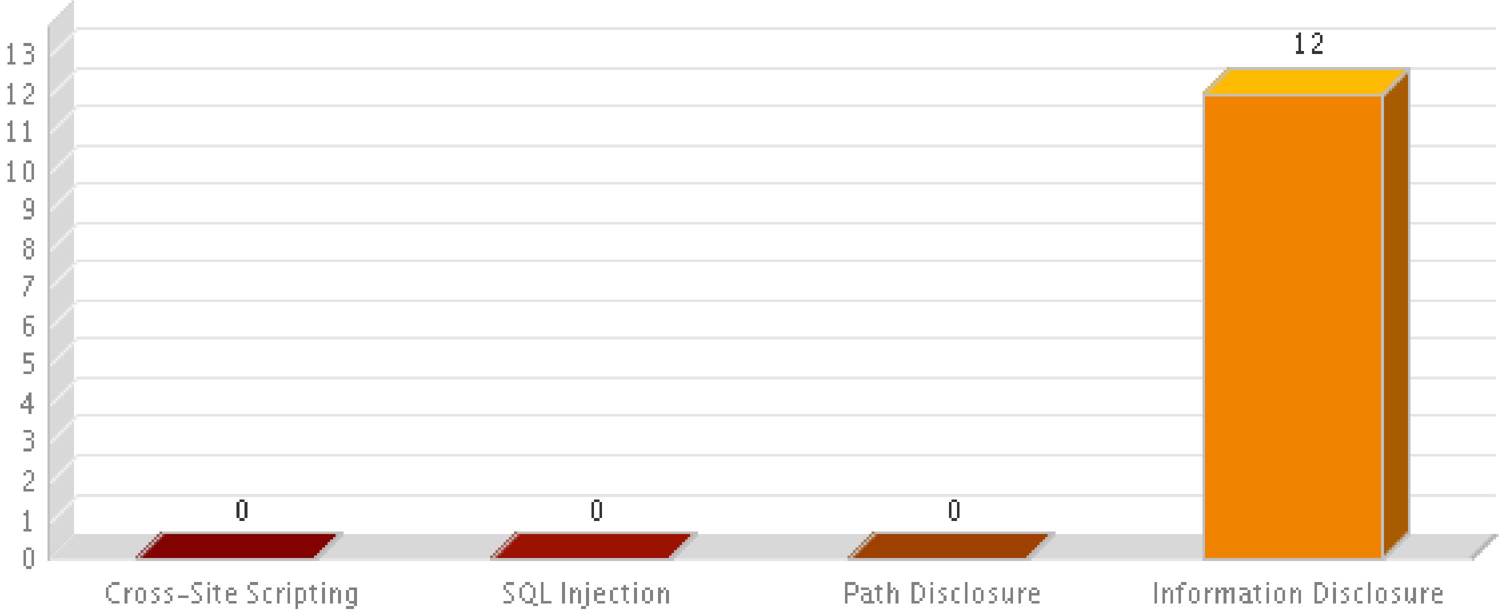
Findings by Severity



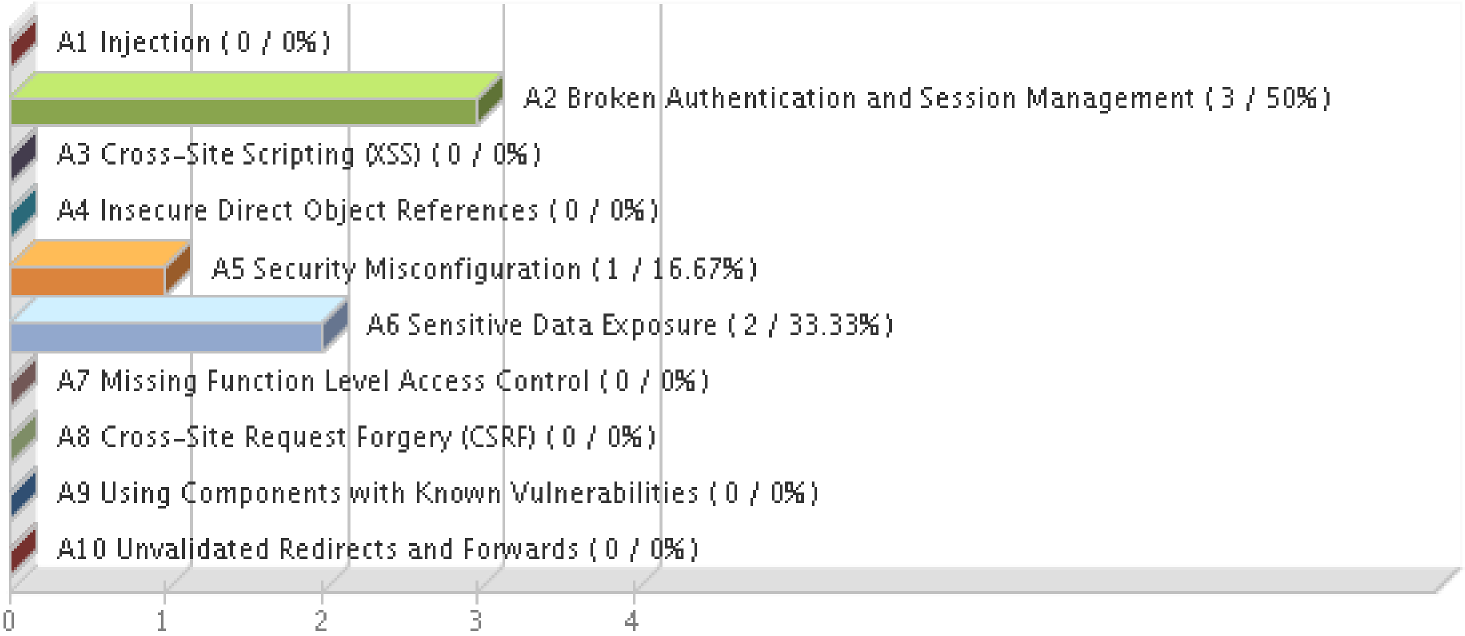
CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free.

WAS Scan Report

Vulnerabilities by Group



OWASP Top 10 2013 Vulnerabilities



Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Relaunch Relaunch Relaunch Relaunch Relaunch WAS_DIME2	11 Aug 2017 09:53 GMT-0500	0	1	5	3	3	0	16

CONFIDENTIAL AND PROPRIETARY INFORMATION.
Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free.

WAS Scan Report

Results(28)

Vulnerability (12)

Information Disclosure (12)

150053 Login Form Is Not Submitted Via HTTPS (1)

150053 Login Form Is Not Submitted Via HTTPS

URL: http://190.144.144.252/DIME/Account/Login

Finding #	**7174512**(569625686)	**Severity**	Confirmed Vulnerability - Level 4
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	A2 Broken Authentication and Session Management A6 Sensitive Data Exposure	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	8.5	**CVSS Temporal**	7.2

Details

Threat
The login form's default action contains a link that is not submitted via HTTPS (HTTP over SSL).

Impact
Sensitive data such as authentication credentials should be encrypted when transmitted over the network. Otherwise they are exposed to sniffing attacks.

Solution
Change the login form's action to submit via HTTPS.

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

Payload	N/A
Request	POST http://190.144.144.252/DIME/Account/Login

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

comment: Parent URL of Login Form is : http://190.144.144.252/DIME/Account/Login
Login Form Is Not Submitted Via HTTPS

150085 Slow HTTP POST vulnerability (1)

150085 Slow HTTP POST vulnerability

URL: http://190.144.144.252/DIME/AdminUsuarios/AccesosUsuarios#/ventanaPrincipal

Finding #	**7174517**(569625691)	**Severity**	Potential Vulnerability - Level 3
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	A5 Security Misconfiguration	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	6.8	**CVSS Temporal**	6.1

Details

Threat

The web application is possibly vulnerable to a "slow HTTP POST" Denial of Service (DoS) attack. This is an application-level DoS that consumes server resources by maintaining open connections for an extended period of time by slowly sending traffic to the server. If the server maintains too many connections open at once, then it may not be able to respond to new, legitimate connections. Unlike bandwidth-consumption DoS attacks, the "slow" attack does not require a large amount of traffic to be sent to the server -- only that the client is able to maintain open connections for several minutes at a time.

The attack holds server connections open by sending properly crafted HTTP POST headers that contain a Content-Length header with a large value to inform the web server how much of data to expect. After the HTTP POST headers are fully sent, the HTTP POST message body is sent at slow speeds to prolong the completion of the connection and lock up server resources. By waiting for the complete request body, the server is helping clients with slow or intermittent connections to complete requests, but is also exposing itself to abuse.

Further information can be found under BlackHat_DC_2011_Brennan_Denial_Service-Slides.pdf.

Impact

All other services remain intact but the web server itself becomes inaccessible.

Solution

Solution would be server-specific, but general recommendations are: - to limit the size of the acceptable request to each form requirements - establish minimal acceptable speed rate - establish absolute request timeout for connection with POST request Server-specific details can be found here. A tool that demonstrates this vulnerability in a more intrusive manner is available here.

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

Payload	N/A
Request	POST http://190.144.144.252/DIME/AdminUsuarios/AccesosUsuarios#/ventanaPrincipal

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

```
Vulnerable to slow HTTP POST attack
 Connection with partial POST body remained open for: 133613 milliseconds
 Server resets timeout after accepting request data from peer.
```

150124 Clickjacking - Framable Page (3)

150124 Clickjacking - Framable Page

URL: http://190.144.144.252/DIME/Account/RecordarContrasena

Finding #	**7174508**(569625682)	Severity	Confirmed Vulnerability - Level 3
Group	Information Disclosure	First Time Detected	11 Aug 2017 09:53 GMT-0500
CWE	-	Last Time Detected	11 Aug 2017 09:53 GMT-0500
OWASP	-	Last Time Tested	11 Aug 2017 09:53 GMT-0500
WASC	-	Times Detected	1
CVSS Base	6.4	CVSS Temporal	5.8

Details

Threat

The page can be easily framed. Anti-framing measures are not used.

Impact

Clickjacking and Cross-Site Request Forgery (CSRF) can be performed by framing the target site. An attack can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

Solution

Two of the most popular prevention are: X-Frame-Options: This header works with modern browsers and can be used to prevent framing of the page. Note that is must be an HTTP header, the setting is ignored if it is created as an "http-equiv" meta element within the page. Framekiller: JavaScript code that prevents the malicious user from framing the page.

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

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/RecordarContrasena

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 URI was framed.

150124 Clickjacking - Framable Page

URL: http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=

Finding #	**7174510**(569625684)	**Severity**	Confirmed Vulnerability - Level 3
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	-	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	6.4	**CVSS Temporal**	5.8

Details

Threat

The page can be easily framed. Anti-framing measures are not used.

Impact

Clickjacking and Cross-Site Request Forgery (CSRF) can be performed by framing the target site. An attack can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

Solution

Two of the most popular prevention are: X-Frame-Options: This header works with modern browsers and can be used to prevent framing of the page. Note that is must be an HTTP header, the setting is ignored if it is created as an "http-equiv" meta element within the page. Framekiller: JavaScript code that prevents the malicious user from framing the page.

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

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=

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 URI was framed.

150124 Clickjacking - Framable Page

URL: http://190.144.144.252/DIME/Account/ObtenerRecordarContra

Finding #	**7174518**(569625692)	**Severity**	Confirmed Vulnerability - Level 3
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	-	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	6.4 **CVSS Temporal**5.8		

Details

Threat

The page can be easily framed. Anti-framing measures are not used.

Impact

Clickjacking and Cross-Site Request Forgery (CSRF) can be performed by framing the target site. An attack can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

Solution

Two of the most popular prevention are: X-Frame-Options: This header works with modern browsers and can be used to prevent framing of the page. Note that is must be an HTTP header, the setting is ignored if it is created as an "http-equiv" meta element within the page. Framekiller: JavaScript code that prevents the malicious user from framing the page.

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

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/ObtenerRecordarContra

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 URI was framed.

150161 Session Cookie Does Not Contain the "Secure" Attribute (1)

150161 Session Cookie Does Not Contain the "Secure" Attribute

URL: http://190.144.144.252/DIME/Account/Login

Finding #	**7174515**(569625689)	**Severity**	Confirmed Vulnerability - Level 3
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	-	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	-	**CVSS Temporal**	-

Details

Threat

The session cookie does not contain the "secure" attribute

Impact

Session Cookies with "secure" attribute are only permitted to be sent via HTTPS. Session cookies sent via HTTP expose users to sniffing attacks that could lead to user impersonation or account compromise

Solution

Apply the "secure" attribute to session cookies to ensure that they will be sent via HTTPS only.

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

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/Login

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

```
ASP.NET_SessionId=cy451rf10seghdwnkm4jkjgp; path=/; domain=190.144.144.252; httponly
```

150122 Cookie Does Not Contain The "secure" Attribute (1)

150122 Cookie Does Not Contain The "secure" Attribute

URL: http://190.144.144.252/DIME/Account/Login

Finding #	**7174514**(569625688)	**Severity**	Confirmed Vulnerability - Level 2
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	A2 Broken Authentication and Session Management A6 Sensitive Data Exposure	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	6.4	**CVSS Temporal**	5.8

Details

Threat

The cookie does not contain the "secure" attribute.

Impact

Cookies with the "secure" attribute are only permitted to be sent via HTTPS. Cookies sent via HTTP expose an unsuspecting user to sniffing attacks that could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "secure" attribute to cookies and force all sensitive requests to be sent via HTTPS.

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

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/Login

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

```
__RequestVerificationToken_L0RJTUU1=aFjlYjQMmK785dWDH3sldgv68ivne71cCkeA858_QEJA05HrpW6X4kTZnCP4kmY9jeO2tUdJKpo6ESxVYQxU_AXoesTlkKAufEHhMkzSi881; path=/;
domain=190.144.144.252; httponly
```

150123 Cookie Does Not Contain The "HTTPOnly" Attribute (1)

150123 Cookie Does Not Contain The "HTTPOnly" Attribute

URL: http://190.144.144.252/DIME/Account/Login

Finding #	**7174513**(569625687)	**Severity**	Confirmed Vulnerability - Level 2
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	A2 Broken Authentication and Session Management	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	-	**CVSS Temporal**	-

Details

Threat

The cookie does not contain the "HTTPOnly" attribute.

Impact

Cookies without the "HTTPOnly" attribute are permitted to be accessed via JavaScript. Cross-site scripting attacks can steal cookies which could lead to user impersonation or compromise of the application account.

Solution

If the associated risk of a compromised account is high, apply the "HTTPOnly" attribute to cookies.

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

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/Login

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

pIntento=1; path=/; domain=190.144.144.252

150159 Session Cookie Set over Non-HTTPS Connection (1)

🟥🟥⬜⬜⬜ 150159 Session Cookie Set over Non-HTTPS Connection

URL: http://190.144.144.252/DIME/Account/Login

Finding #	**7174516**(569625690)	**Severity**	Confirmed Vulnerability - Level 2
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	-	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	- **CVSS Temporal**-		

Details

Threat

Session cookie set over Non-HTTPS connection

Impact

Session cookie set over Non-HTTPS connection can lead to a Man in the Middle attack and cookie data can be stolen. Cookie values can be sniffed by an attacker. This later can be used to impersonate the authenticated user and gain unauthorized access.

Solution

The general recommendation is to set the Session cookie over HTTPS (secure connection)

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

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/Login

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

```
ASP.NET_SessionId=cy451rf10seghdwnkm4jkjgp; path=/; domain=190.144.144.252; httponly
```

🟨⬜⬜⬜⬜ 150081 Clickjacking - X-Frame-Options header is not set (3)

150081 Clickjacking - X-Frame-Options header is not set

URL: http://190.144.144.252/DIME/Account/RecordarContrasena

Finding #	**7174509**(569625683)	**Severity**	Potential Vulnerability - Level 1
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	-	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	5 **CVSS Temporal**4.1		

Details

Threat

X-Frame-Options header is not set, and that may lead to a possible framing of the page. An attacker can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

Impact

Attacks like Clickjacking and Cross-Site Request Forgery (CSRF) could be performed.

Solution

Set the X-Frame-Options: This header works with modern browsers and can be used to prevent framing of the page. Note that it must be an HTTP header, the setting is ignored if it is created as an "http-equiv" meta element within the page.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

```
http://190.144.144.252/DIME/AdminUsuarios/AccesosUsuarios#/ventanaPrincipal
http://190.144.144.252/DIME/Account/Login
```

Payloads

#1 Request

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/RecordarContrasena

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

▮▯▯▯▯ 150081 Clickjacking - X-Frame-Options header is not set

URL: http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=

Finding #	**7174511**(569625685)	**Severity**	Potential Vulnerability - Level 1
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	-	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	5	**CVSS Temporal**	4.1

Details

Threat

X-Frame-Options header is not set, and that may lead to a possible framing of the page. An attacker can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

Impact

Attacks like Clickjacking and Cross-Site Request Forgery (CSRF) could be performed.

Solution

Set the X-Frame-Options: This header works with modern browsers and can be used to prevent framing of the page. Note that it must be an HTTP header, the setting is ignored if it is created as an "http-equiv" meta element within the page.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

```
http://190.144.144.252/DIME/AdminUsuarios/AccesosUsuarios#/ventanaPrincipal
http://190.144.144.252/DIME/Account/Login
http://190.144.144.252/DIME/Account/RecordarContrasena
```

Payloads

#1 Request

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=

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

150081 Clickjacking - X-Frame-Options header is not set

URL: http://190.144.144.252/DIME/Account/ObtenerRecordarContra

Finding #	**7174519**(569625693)	**Severity**	Potential Vulnerability - Level 1
Group	Information Disclosure	**First Time Detected**	11 Aug 2017 09:53 GMT-0500
CWE	-	**Last Time Detected**	11 Aug 2017 09:53 GMT-0500
OWASP	-	**Last Time Tested**	11 Aug 2017 09:53 GMT-0500
WASC	-	**Times Detected**	1
CVSS Base	5 **CVSS Temporal**4.1		

Details

Threat

X-Frame-Options header is not set, and that may lead to a possible framing of the page. An attacker can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

Impact

Attacks like Clickjacking and Cross-Site Request Forgery (CSRF) could be performed.

Solution

Set the X-Frame-Options: This header works with modern browsers and can be used to prevent framing of the page. Note that it must be an HTTP header, the setting is ignored if it is created as an "http-equiv" meta element within the page.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

http://190.144.144.252/DIME/AdminUsuarios/AccesosUsuarios#/ventanaPrincipal
http://190.144.144.252/DIME/Account/Login
http://190.144.144.252/DIME/Account/RecordarContrasena

Payloads

#1 Request

Payload	N/A
Request	GET http://190.144.144.252/DIME/Account/ObtenerRecordarContra

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

Information Gathered (16)

Information Gathered (16)

45017 Operating System Detected (1)

45017 Operating System Detected

Finding #	**3042782**(569625679)	**Severity**	Information Gathered - Level 2
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 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.

Results

Operating System	Technique	ID
Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8	TCP/IP Fingerprint	U2514:80

150018 Connection Error Occurred During Web Application Scan (1)

150018 Connection Error Occurred During Web Application Scan

Finding #	**3042769**(569625666)	**Severity**	Information Gathered - Level 2
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 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: 16
Links with highest number of timeouts:
 1 http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=%2525%7B%28%23_%3D%27multipart%2fform-data%27%29.%28%23dm
%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B
%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28@com.opensymphony.xwork2.ognl.OgnlUtil@class
%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%
 1 http://190.144.144.252/DIME/Account/Login
 1 http://190.144.144.252/DIME/Account/RecordarContrasena
 1 http://190.144.144.252/DIME/favicon.ico?method:%23_memberAccess%3d%40ognl.OgnlContext%20%40DEFAULT_MEMBER_ACCESS%2c%23a%3d%40java.lang.Runtime%40getRuntime
%28%29.exec%28%23parameters.command%20%5B0%5D%29.getInputStream%28%29%2c%23b%3dnew%20java.io.InputStreamReader%28%23a%29%2c%23c%3dnew
%20%20java.io.BufferedReader%28%23b%29%2c%23d%3dnew%20char%5B51020%5D%2c%23c.read%28%23d%29%2c%23kxlzx%3d%20%40org.apache.struts2.ServletActionContext
%40getResponse%28%29.getWriter%28%29%2c%23kxlzx.println%28%23d%20%29
 1 http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=%25%7B%28%23_%3D%27multipart%2fform-data%27%29.%28%23dm
%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B
%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28@com.opensymphony.xwork2.ognl.OgnlUtil@class
%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28
 1 http://190.144.144.252/DIME/Account/ObtenerRecordarContra
 1 http://190.144.144.252/DIME/favicon.ico?method:%23_memberAccess%3d%40ognl.OgnlContext%20%40DEFAULT_MEMBER_ACCESS%2c%23a%3d%40java.lang.Runtime%40getRuntime
%28%29.exec%28%23parameters.command%20%5B0%5D%29.getInputStream%28%29%2c%23b%3dnew%20java.io.InputStreamReader%28%23a%29%2c%23c%3dnew
%20%20java.io.BufferedReader%28%23b%29%2c%23d%3dnew%20char%5B51020%5D%2c%23c.read%28%23d%29%2c%23kxlzx%3d%20%40org.apache.struts2.ServletActionContext
%40getResponse%28%29.getWriter%28%29%2c%23kxlzx.println%28%23d%20%29
 1 http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=
 1 http://190.144.144.252/DIME/AdminLTE/plugins/ionicons/fonts/ionicons.ttf?v=2.0.0
 1 http://190.144.144.252/DIME/AdminLTE/plugins/ionicons/fonts/ionicons.ttf?v=%2525%7B%28%23_%3D%27multipart%2fform-data%27%29.%28%23dm
%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B
%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28@com.opensymphony.xwork2.ognl.OgnlUtil@class
%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExclud
 1 http://190.144.144.252/DIME/AdminLTE/plugins/fonts/fontawesome-webfont.ttf?v=4.5.0
 1 http://190.144.144.252/DIME/AdminLTE/plugins/fonts/fontawesome-webfont.ttf?v=%2525%7B%28%23_%3D%27multipart%2fform-data%27%29.%28%23dm
%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B
%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28@com.opensymphony.xwork2.ognl.OgnlUtil@class
%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcl
 1 http://190.144.144.252/DIME/AdminLTE/plugins/ionicons/fonts/ionicons.ttf?v=%25%7B%28%23_%3D%27multipart%2fform-data%27%29.%28%23dm
%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B
%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28@com.opensymphony.xwork2.ognl.OgnlUtil@class
%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcluded
 1 http://190.144.144.252/favicon.ico?method:%23_memberAccess%3d%40ognl.OgnlContext%20%40DEFAULT_MEMBER_ACCESS%2c%23a%3d%40java.lang.Runtime%40getRuntime
%28%29.exec%28%23parameters.command%20%5B0%5D%29.getInputStream%28%29%2c%23b%3dnew%20java.io.InputStreamReader%28%23a%29%2c%23c%3dnew
%20%20java.io.BufferedReader%28%23b%29%2c%23d%3dnew%20char%5B51020%5D%2c%23c.read%28%23d%29%2c%23kxlzx%3d%20%40org.apache.struts2.ServletActionContext
%40getResponse%28%29.getWriter%28%29%2c%23kxlzx.println%28%23d%20%29%2c%2
```

```
 1 http://190.144.144.252/favicon.ico?method:%23_memberAccess%3d%40ognl.OgnlContext%20%40DEFAULT_MEMBER_ACCESS%2c%23a%3d%40java.lang.Runtime%40getRuntime
%28%29.exec%28%23parameters.command%20%5B0%5D%29.getInputStream%28%29%2c%23b%3dnew%20java.io.InputStreamReader%28%23a%29%2c%23c%3dnew
%20%20java.io.BufferedReader%28%23b%29%2c%23d%3dnew%20char%5B51020%5D%2c%23c.read%28%23d%29%2c%23kxlzx%3d%20%40org.apache.struts2.ServletActionContext
%40getResponse%28%29.getWriter%28%29%2c%23kxlzx.println%28%23d%20%29%2c%2
 1 http://190.144.144.252/DIME/AdminLTE/plugins/fonts/fontawesome-webfont.ttf?v=%25%7B%28%23_%3D%27multipart%2fform-data%27%29.%28%23dm
%3D@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B
%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28@com.opensymphony.xwork2.ognl.OgnlUtil@class
%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExclud

Phase wise summary of timeout and connection errors encountered:
ePhaseParameterTests : 6 0
ePhaseShellShock : 6 0
ePhasePathTests : 4 0
```

6 DNS Host Name (1)

6 DNS Host Name

Finding #	**3042773**(569625670)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 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.

Results

IP address	Host name
190.144.144.252	No registered hostname

45038 Host Scan Time (1)

45038 Host Scan Time

Finding #	**3042779**(569625676)	Severity	Information Gathered - Level 1
Group	Information Gathered	Detection Date	11 Aug 2017 09:53 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: 2596 seconds

Start time: Fri, Aug 11 2017, 14:53:34 GMT

End time: Fri, Aug 11 2017, 15:36:50 GMT
```

150008 Web Application Authentication Failed (1)

150008 Web Application Authentication Failed

Finding #	**3042783**(569625680)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Web application authentication was enabled during the scan, but login attempts using the authentication credentials specified in the Web application's authentication record for this host failed.

Impact

Vulnerabilities that require Web application authentication may not be detected.

Solution

Verify that the authentication credentials defined in the Web application's authentication record are valid for this host.

Results

```
Auth failed against form: http://190.144.144.252/DIME/Account/Login
Web Application Authentication Record: Form Auth Record AUTH_DIME, #469310
User Name: 1032411326
```

150009 Links Crawled (1)

150009 Links Crawled

Finding #	**3042784**(569625681)	Severity	Information Gathered - Level 1
Group	Information Gathered	Detection Date	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of unique links crawled and HTML forms submitted by the Web application scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined at scan launch. The maximum links to crawl includes links in this list and requests for the same link made as an anonymous and authenticated user.

Impact

N/A

Solution

N/A

Results

```
Duration of crawl phase (seconds): 171.00
Number of links: 12
(This number excludes form requests and links re-requested during authentication.)

http://190.144.144.252/DIME/Account/Login
http://190.144.144.252/DIME/Account/ObtenerRecordarContra
http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=
http://190.144.144.252/DIME/Account/RecordarContrasena
http://190.144.144.252/DIME/AdminLTE/plugins/fonts/fontawesome-webfont.ttf?v=4.5.0
http://190.144.144.252/DIME/AdminLTE/plugins/ionicons/fonts/ionicons.ttf?v=2.0.0
http://190.144.144.252/DIME/AdminLTEplugins/ichecwk/css/sqare/blue
http://190.144.144.252/DIME/Home/DashboardAsesor
http://190.144.144.252/DIME/Scripts/Account/Login
http://190.144.144.252/DIME/Scripts/Home/DashboardV2
http://190.144.144.252/DIME/favicon.ico
http://190.144.144.252/favicon.ico
```

150010 External Links Discovered (1)

150010 External Links Discovered

Finding #	**3042781**(569625678)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The external links discovered by the Web application scanning engine are provided in the Results section. These links were present on the target Web application, but were not crawled.

Impact

N/A

Solution

N/A

Results

```
Number of links: 4
https://oss.maxcdn.com/html5shiv/3.7.3/html5shiv.min.js
https://oss.maxcdn.com/respond/1.4.2/respond.min.js
https://l2.io/ip.js?var=userip
http://go.microsoft.com/fwlink/?linkid=66138&clcid=0x409
```

150021 Scan Diagnostics (1)

150021 Scan Diagnostics

Finding #	**3042775**(569625672)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 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.
Collected 29 links overall in 0 hours 2 minutes 51 seconds duration.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 4) + files:(0 x 12) + directories:(9 x 18) + paths:(0 x 30) = total (162)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 30 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 162 requests, 3 seconds. Completed 162 requests of 162 estimated requests (100%). All tests completed.
Batch #0 WS enumeration: estimated time < 1 minute (10 tests, 28 inputs)
WS enumeration: 10 vulnsigs tests, completed 160 requests, 4 seconds. Completed 160 requests of 280 estimated requests (57.1429%). All tests completed.
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (50 tests, 2 inputs)
Batch #1 URI parameter manipulation (no auth): 50 vulnsigs tests, completed 98 requests, 606 seconds. Completed 98 requests of 100 estimated requests (98%). All tests completed.
Batch #1 Form parameter manipulation (no auth): estimated time < 1 minute (50 tests, 12 inputs)
Batch #1 Form parameter manipulation (no auth): 50 vulnsigs tests, completed 442 requests, 64 seconds. Completed 442 requests of 600 estimated requests (73.6667%). All tests completed.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 2 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 48 requests, 3 seconds. Completed 48 requests of 48 estimated requests (100%). All tests completed.
Batch #1 Form blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 12 inputs)
Batch #1 Form blind SQL manipulation (no auth): 8 vulnsigs tests, completed 144 requests, 24 seconds. Completed 144 requests of 288 estimated requests (50%). All tests completed.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (11 tests, 2 inputs)
Batch #1 URI parameter time-based tests (no auth): 11 vulnsigs tests, completed 22 requests, 3 seconds. Completed 22 requests of 22 estimated requests (100%). All tests completed.
Batch #1 Form field time-based tests (no auth): estimated time < 1 minute (11 tests, 12 inputs)
Batch #1 Form field time-based tests (no auth): 11 vulnsigs tests, completed 99 requests, 17 seconds. Completed 99 requests of 132 estimated requests (75%). All tests completed.
Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (50 tests, 1 inputs)
Batch #2 URI parameter manipulation (no auth): 50 vulnsigs tests, completed 49 requests, 302 seconds. Completed 49 requests of 50 estimated requests (98%). All tests completed.
Batch #2 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 1 inputs)
Batch #2 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 32 requests, 1 seconds. Completed 32 requests of 24 estimated requests (133.333%). All tests completed.
Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (11 tests, 1 inputs)
Batch #2 URI parameter time-based tests (no auth): 11 vulnsigs tests, completed 11 requests, 2 seconds. Completed 11 requests of 11 estimated requests (100%). All tests completed.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 DOM XSS exploitation: 1 vulnsigs tests, completed 0 requests, 61 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (33 tests, 0 inputs)
Batch #4 HTTP call manipulation: 33 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 Open Redirect analysis: 1 vulnsigs tests, completed 0 requests, 0 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, 13 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 13 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 10 minutes (37 tests, 3 inputs)
Batch #4 Cookie manipulation: 37 vulnsigs tests, completed 822 requests, 35 seconds. Completed 822 requests of 783 estimated requests (104.981%). XSS optimization removed 72 links. All tests completed.
Batch #4 Header manipulation: estimated time < 1 minute (37 tests, 9 inputs)
Batch #4 Header manipulation: 37 vulnsigs tests, completed 220 requests, 16 seconds. Completed 220 requests of 450 estimated requests (48.8889%). XSS optimization removed 216 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 11 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 6 requests, 600 seconds. Completed 6 requests of 11 estimated requests (54.5455%). Some tests were skipped due to errors.
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, 11 inputs)
Batch #4 httpoxy detector: 1 vulnsigs tests, completed 11 requests, 1 seconds. Completed 11 requests of 11 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 Login Brute Force manipulation: estimated time < 1 minute (188 tests, 1 inputs)
Batch #4 Login Brute Force manipulation: 188 vulnsigs tests, completed 188 requests, 293 seconds. Completed 188 requests of 188 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 200 requests, 17 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 4) + files:(15 x 12) + directories:(104 x 18) + paths:(18 x 30) = total (2608)
Batch #5 Path manipulation: estimated time < 10 minutes (141 tests, 30 inputs)
Batch #5 Path manipulation: 141 vulnsigs tests, completed 2220 requests, 353 seconds. Completed 2220 requests of 2608 estimated requests (85.1227%). All tests completed.
Total requests made: 5088
Average server response time: 0.20 seconds
Most recent links:
First column indicates HTTP response code,
 Special cases:
 -TO: The request timed out
 -CE: The request did not complete due to connection error):
404 http://190.144.144.252/DIME/AdminLTE/plugins/system/
404 http://190.144.144.252/DIME/AdminLTE/system/
404 http://190.144.144.252/DIME/AdminLTE/plugins/ionicons/system/
404 http://190.144.144.252/DIME/AdminLTE/plugins/ionicons/fonts/system/
404 http://190.144.144.252/DIME/Scripts/system/
404 http://190.144.144.252/DIME/Scripts/Home/system/
404 http://190.144.144.252/DIME/Scripts/Account/system/
404 http://190.144.144.252/DIME/AdminLTE/plugins/fonts/system/
404 http://190.144.144.252/DIME/Resources/system/
404 http://190.144.144.252/DIME/Resources/Images/system/
```

150028 Cookies Collected (1)

150028 Cookies Collected

Finding #	**3042778**(569625675)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were received from the web application 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: 3
__RequestVerificationToken_L0RJTUU1=aFjlYjQMmK785dWDH3sldgv68ivne71cCkeA858_QEJA05HrpW6X4kTZnCP4kmY9jeO2tUdJKpo6ESxVYQxU_AXoesTlkKAufEHhMkzSi881;
HttpOnly; path=/ First set at URL: http://190.144.144.252/DIME/Account/Login
pIntento=1; path=/ First set at URL: http://190.144.144.252/DIME/Account/Login
ASP.NET_SessionId=cy451rf10seghdwnkm4jkjgp; HttpOnly; path=/ First set at URL: http://190.144.144.252/DIME/Account/Login
```

150082 Protection against Clickjacking vulnerability (1)

150082 Protection against Clickjacking vulnerability

Finding #	**3042770**(569625667)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The URIs listed have a protection against Clickjacking. The protection is implemented by use of X-Frame-Options header.

Impact

X-Frame-Options header is used to prevent framing of the page.

Solution

Another technique of prevention against Clickjacking is the "framekiller" JavaScript.

Results

http://190.144.144.252/DIME/Account/Login

150099 Cookies Issued Without User Consent (1)

150099 Cookies Issued Without User Consent

Finding #	**3042780**(569625677)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 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
__RequestVerificationToken_L0RJTUU1=w2DjH5BLE4Y3uqC1pqNI2x57DkRvxV7vyAlf1c0KOrnmEsje_xiocFavCFmVDOJabJI5VppIVlq6M4lDGipFa6dQwKtpFerjT_MfMyXz2Ok1; HttpOnly;
path=/ First set at URL: http://190.144.144.252/DIME/Account/Login
```

150115 Authentication Form found (1)

150115 Authentication Form found

Finding #	**3042771**(569625668)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Authentication Form was found during the web application crawling.

Impact

N/A

Solution

N/A

Results

```
Authentication form found at: http://190.144.144.252/DIME/Account/Login
 Action uri: http://190.144.144.252/DIME/Account/Login
 Fields: __RequestVerificationToken, Cedula, Contrasena,
Authentication form found at: http://190.144.144.252/DIME/Account/Login
 Action uri: http://190.144.144.252/DIME/Account/Login
 Fields: __RequestVerificationToken, Cedula, Contrasena,
Authentication form found at: http://190.144.144.252/DIME/Account/Login
 Action uri: http://190.144.144.252/DIME/Account/Login
 Fields: __RequestVerificationToken, Cedula, Contrasena,
```

150126 Links With High Resource Consumption (1)

150126 Links With High Resource Consumption

Finding #	**3042777**(569625674)	Severity	Information Gathered - Level 1
Group	Information Gathered	Detection Date	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

Impact

The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

Solution

Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

Results

```
8160.600000 bytes/sec http://190.144.144.252/DIME/Account/ObtenerRecordarContra
8360.300000 bytes/sec http://190.144.144.252/DIME/Account/ObtenerRecordarContra?cedula=
16103.100000 bytes/sec http://190.144.144.252/DIME/AdminLTEplugins/icheck/css/sqare/blue?v=l3WwYU5UXVLTL5nA65sAOjA5RQDfzclOFm3fsXVqijI1
16191.900000 bytes/sec http://190.144.144.252/favicon.ico
17379.400000 bytes/sec http://190.144.144.252/DIME/AdminLTEplugins/ichecwk/css/sqare/blue
44623.600000 bytes/sec http://190.144.144.252/DIME/Scripts/Home/DashboardV2
45053.900000 bytes/sec http://190.144.144.252/DIME/Scripts/Account/Login
150020.700000 bytes/sec http://190.144.144.252/DIME/favicon.ico
1784931.500000 bytes/sec http://190.144.144.252/DIME/AdminLTE/plugins/fonts/fontawesome-webfont.ttf?v=4.5.0
2410151.200000 bytes/sec http://190.144.144.252/DIME/AdminLTE/plugins/ionicons/fonts/ionicons.ttf?v=2.0.0
```

150148 AJAX Links Crawled (1)

150148 AJAX Links Crawled

Finding #	**3042774**(569625671)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of unique AJAX links crawled by the Web application scanner appear in the Results section. The link can either be a URL with fragment or selenium script. To open the AJAX link with fragment, open it in browser and to open the selenium script, use selenium IDE to run it.

Impact

N/A

Solution

N/A

Results

```
Number of ajax links: 1
http://190.144.144.252/DIME/AdminUsuarios/AccesosUsuarios#/ventanaPrincipal
```

150152 Forms Crawled (1)

150152 Forms Crawled

Finding #	**3042776**(569625673)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list and details of unique forms submitted by the Web application scanner appear in the Results section. This list does not contain authentication forms (i.e. login forms) which are reported separately in QID 150115.

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
```

150176 JavaScript Libraries Detected (1)

150176 JavaScript Libraries Detected

Finding #	**3042772**(569625669)	**Severity**	Information Gathered - Level 1
Group	Information Gathered	**Detection Date**	11 Aug 2017 09:53 GMT-0500
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The JavaScript libraries discovered by the Web Application Scanning engine are provided in the Results section. The discovered libraries are reported only once based on the page of the web application on which they were first detected. These libraries are reported along with other information such as: the page on which they were first found and their version and script uri.

Impact

N/A

Solution

N/A

Results

```
Number of unique JS libraries: 3
Javascript library : Angular
Version : 1.5.8
Script uri : http://190.144.144.252/DIME/AdminLTE/plugins/angular/angular.min.js
Found on the following page(only first page is reported):
 http://190.144.144.252/DIME/Account/RecordarContrasena

================================================================

Javascript library : Bootstrap
Version : 3.3.4
Script uri : http://190.144.144.252/DIME/AdminLTE/bootstrap/js/bootstrap.min.js
Found on the following page(only first page is reported):
 http://190.144.144.252/DIME/Account/Login

================================================================

Javascript library : jQuery
Version : 2.1.4
Script uri : http://190.144.144.252/DIME/AdminLTEplugins/jquery/js?v=gGGRI7xCOnEK-4qvkXXwhmbyGmA8S3tmz-Wto5bGsIc1
Found on the following page(only first page is reported):
 http://190.144.144.252/DIME/Account/Login

================================================================
```

Appendix

Scan Details

Relaunch Relaunch Relaunch Relaunch Relaunch WAS_DIME2

Reference	was/1502463199311.21548289
Date	11 Aug 2017 09:53 GMT-0500
Mode	On-Demand
Type	Vulnerability
Authentication	AUTH_DIME
Scanner Appliance	External (IP: 64.39.99.51, Scanner: 9.5.35-1, WAS: 4.3.82-1, Signatures: 2.4.106-3)
Profile	Profile GSI
DNS Override	-
Duration	00:43:16
Status	Finished
Authentication Status	Failed

Web Application Details: WAS_DIME

Name	WAS_DIME
URL	http://190.144.144.252/DIME/AdminUsuarios/AccesosUsuarios#/ventanaPrincipal
Owner	Alejandro López López (temex_al)
Scope	Limit to URL hostname
Operating System	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8

Severity Levels

Confirmed Vulnerabilities

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

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.**