WEB APPLICATION PENETRATION TESTING

GROUP 2.3

PratheeshKumar.N -20BCI0195

Sandhiya.N -20BCI0196

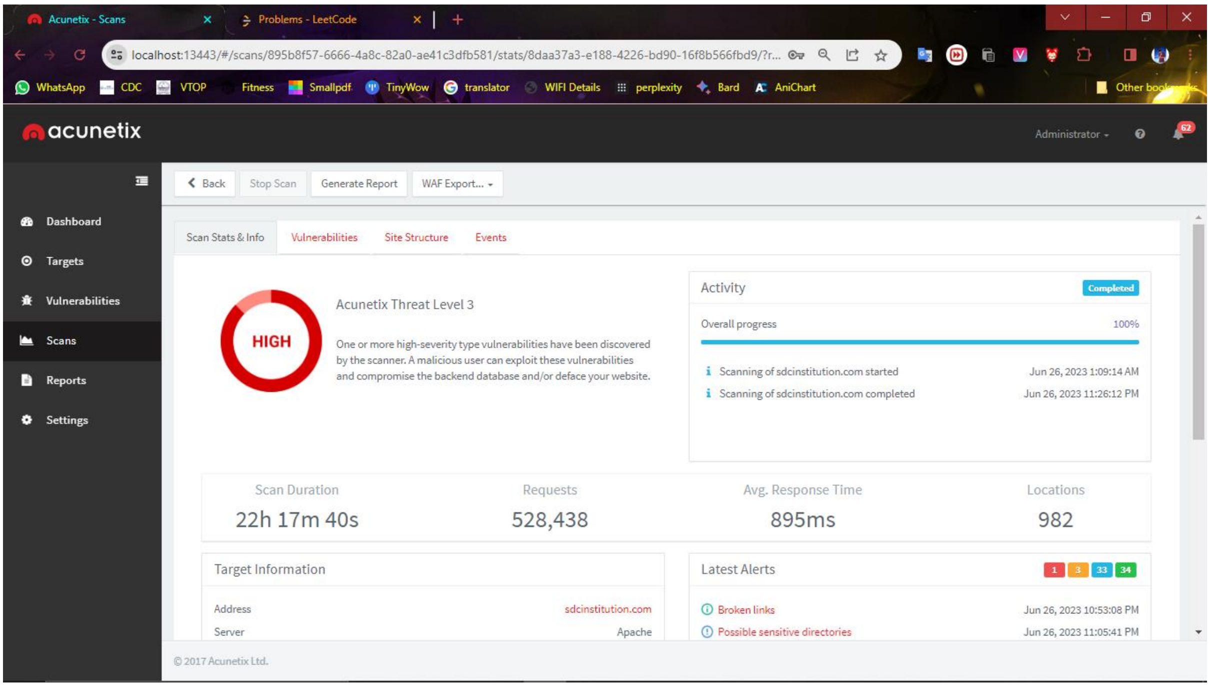
Mukunthan.D-20BCI0291

VULNERABILITY REPORT:

Target Website: http://sdcinstitution.com/

Scanning Tool : Acunetix

Scanning Details :



Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Activity

Overall progress 100%

Scanning of sdcinstitution.com started Jun 26, 2023 1:09:14 AM

Scanning of sdcinstitution.com completed Jun 26, 2023 11:26:12 PM

Scan Duration	Requests	Avg. Response Time	Locations
22h 17m 40s	528,438	895ms	982

Target Information

Address	sdcinstitution.com
Server	Apache

Latest Alerts

Broken links	Jun 26, 2023 10:53:08 PM
Possible sensitive directories	Jun 26, 2023 11:05:41 PM

Scan of http://sdcinstitution.com

Scan details

Scan information	
Start time	26/06/2023, 01:09:11
Start url	http://sdcinstitution.com
Host	http://sdcinstitution.com
Scan time	1337 minutes, 40 seconds
Profile	Full Scan

Threat level

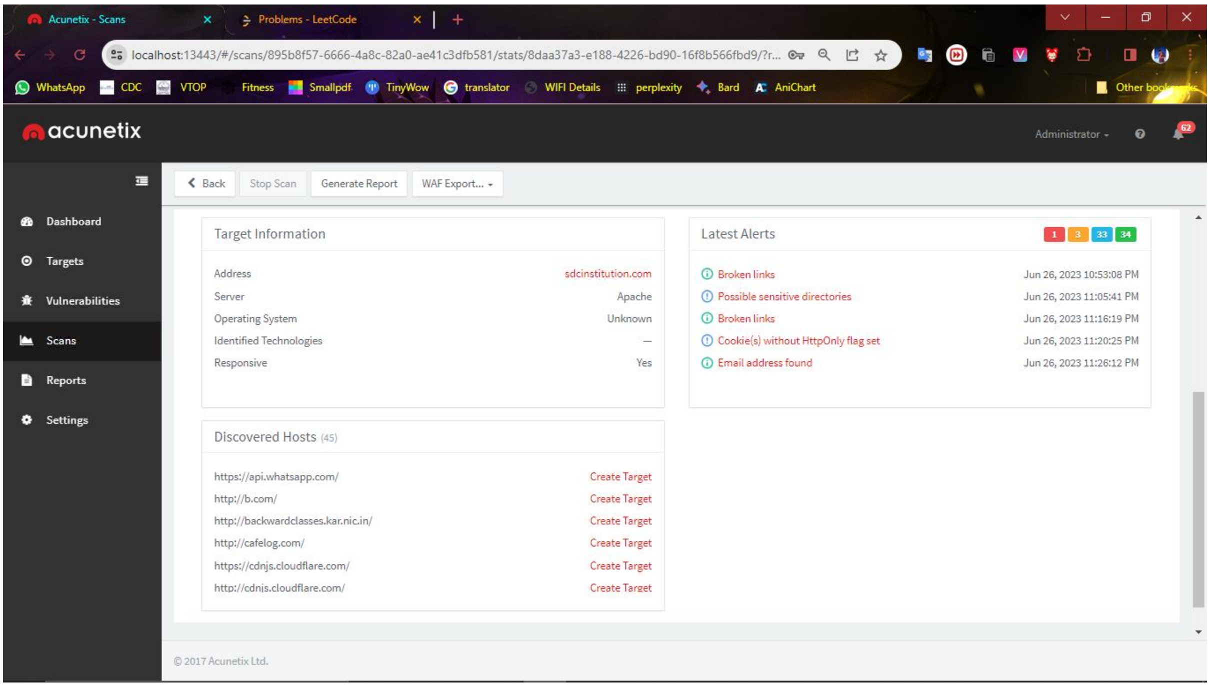
Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	71
High	1
Medium	3
Low	33
Informational	34

Target Information:



Target Information

Address	sdcinstitution.com
Server	Apache
Operating System	Unknown
Identified Technologies	—
Responsive	Yes

Latest Alerts 1 3 33 34

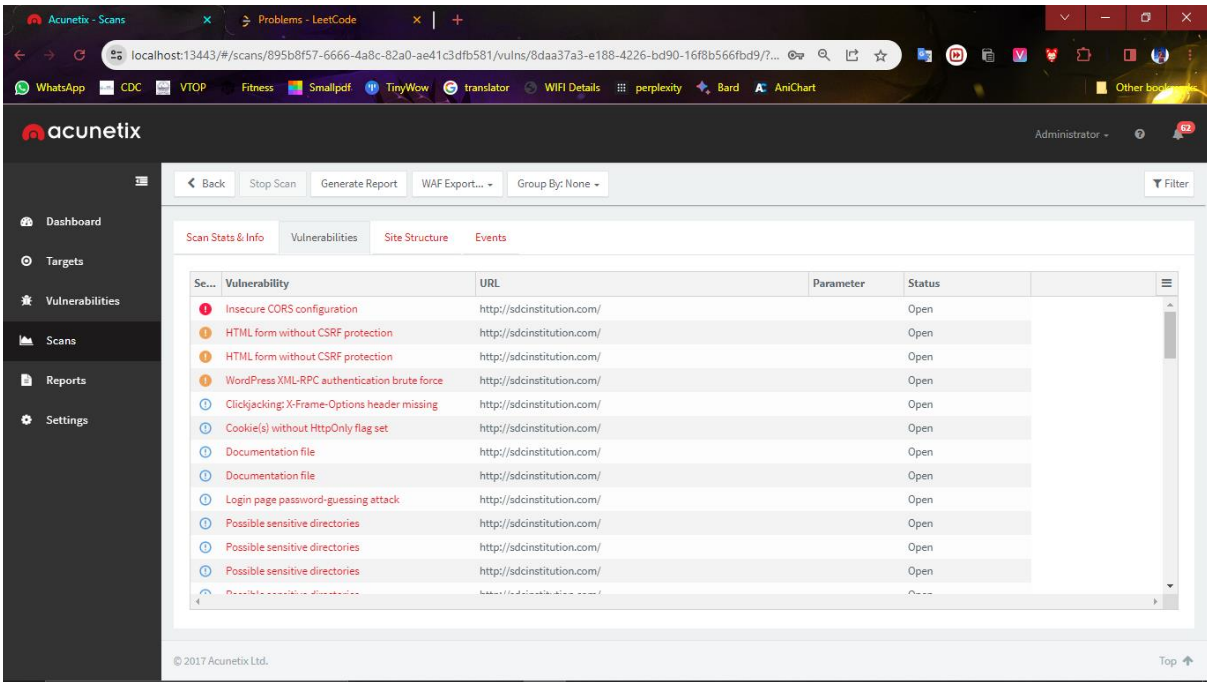
Broken links	Jun 26, 2023 10:53:08 PM
Possible sensitive directories	Jun 26, 2023 11:05:41 PM
Broken links	Jun 26, 2023 11:16:19 PM
Cookie(s) without HttpOnly flag set	Jun 26, 2023 11:20:25 PM
Email address found	Jun 26, 2023 11:26:12 PM

Discovered Hosts (45)

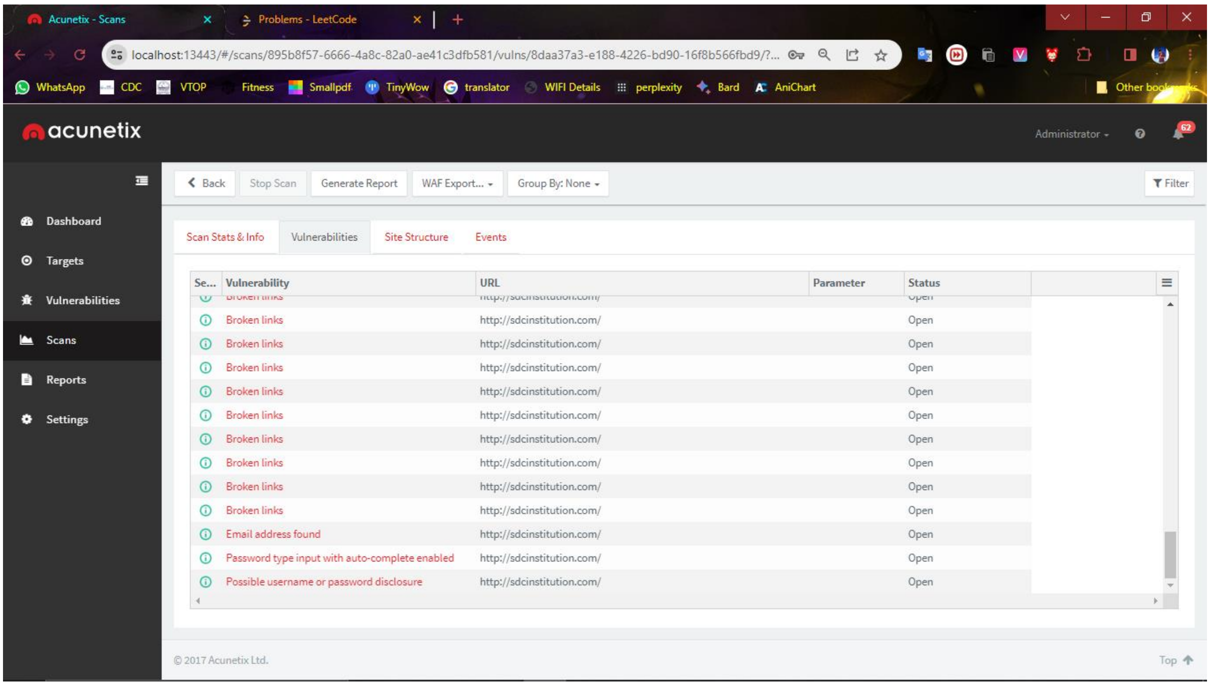
https://api.whatsapp.com/	Create Target
http://b.com/	Create Target
http://backwardclasses.kar.nic.in/	Create Target
http://cafelog.com/	Create Target
https://cdnjs.cloudflare.com/	Create Target
http://cdnjs.cloudflare.com/	Create Target

© 2017 Acunetix Ltd.

Available Vulnerabilities:



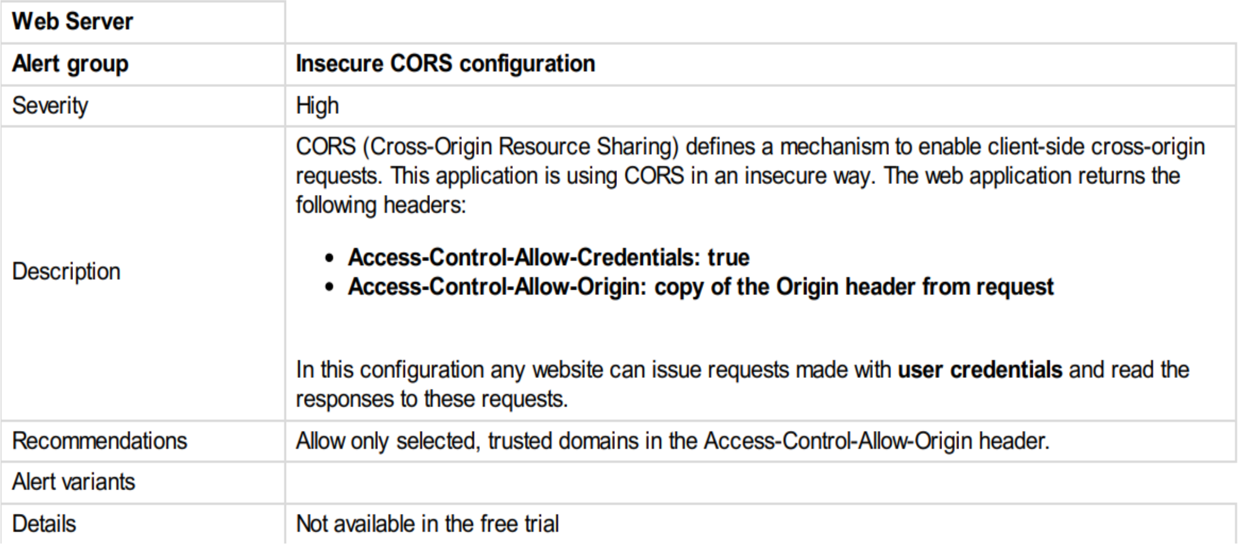
Se...	Vulnerability	URL	Parameter	Status
!	Insecure CORS configuration	http://sdcinstitution.com/		Open
!	HTML form without CSRF protection	http://sdcinstitution.com/		Open
!	HTML form without CSRF protection	http://sdcinstitution.com/		Open
!	WordPress XML-RPC authentication brute force	http://sdcinstitution.com/		Open
ⓘ	Clickjacking: X-Frame-Options header missing	http://sdcinstitution.com/		Open
ⓘ	Cookie(s) without HttpOnly flag set	http://sdcinstitution.com/		Open
ⓘ	Documentation file	http://sdcinstitution.com/		Open
ⓘ	Documentation file	http://sdcinstitution.com/		Open
ⓘ	Login page password-guessing attack	http://sdcinstitution.com/		Open
ⓘ	Possible sensitive directories	http://sdcinstitution.com/		Open
ⓘ	Possible sensitive directories	http://sdcinstitution.com/		Open
ⓘ	Possible sensitive directories	http://sdcinstitution.com/		Open
ⓘ	Possible sensitive directories	http://sdcinstitution.com/		Open



Se...	Vulnerability	URL	Parameter	Status
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Broken links	http://sdcinstitution.com/		Open
ⓘ	Email address found	http://sdcinstitution.com/		Open
ⓘ	Password type input with auto-complete enabled	http://sdcinstitution.com/		Open
ⓘ	Possible username or password disclosure	http://sdcinstitution.com/		Open

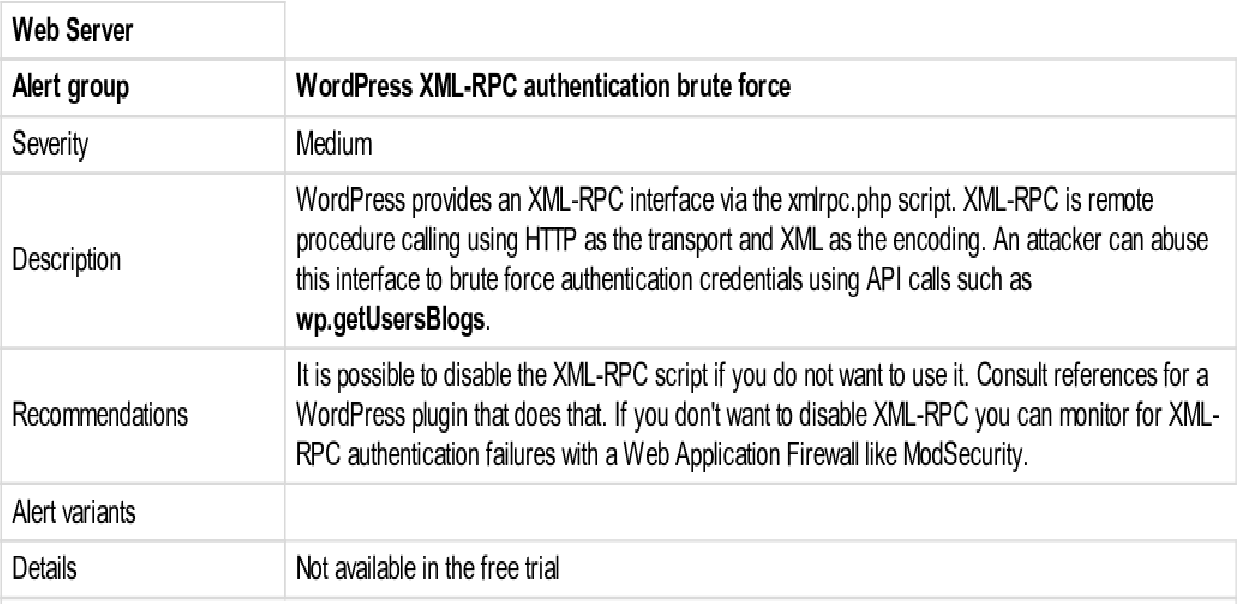
Vulnerbility Details :

1.Insecure CORS configuration



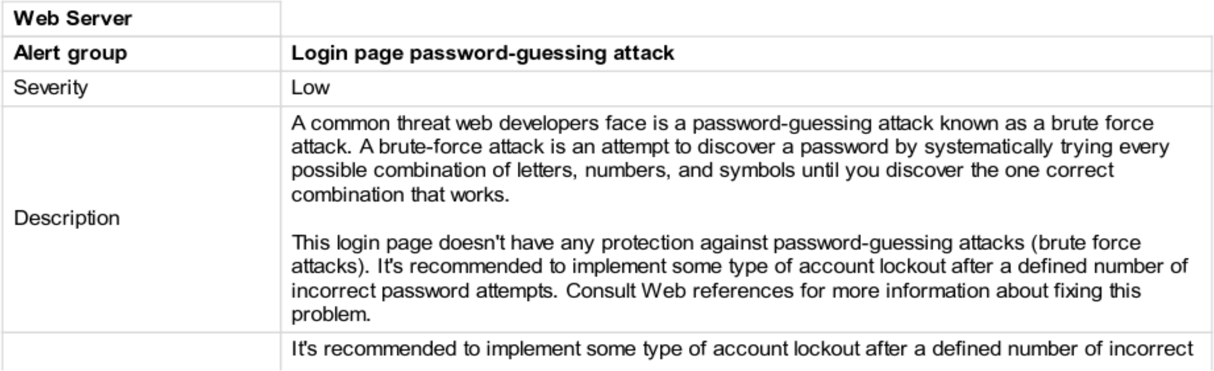
Web Server	
Alert group	**Insecure CORS configuration**
Severity	High
Description	CORS (Cross-Origin Resource Sharing) defines a mechanism to enable client-side cross-origin requests. This application is using CORS in an insecure way. The web application returns the following headers: • **Access-Control-Allow-Credentials: true** • **Access-Control-Allow-Origin: copy of the Origin header from request** In this configuration any website can issue requests made with **user credentials** and read the responses to these requests.
Recommendations	Allow only selected, trusted domains in the Access-Control-Allow-Origin header.
Alert variants	
Details	Not available in the free trial

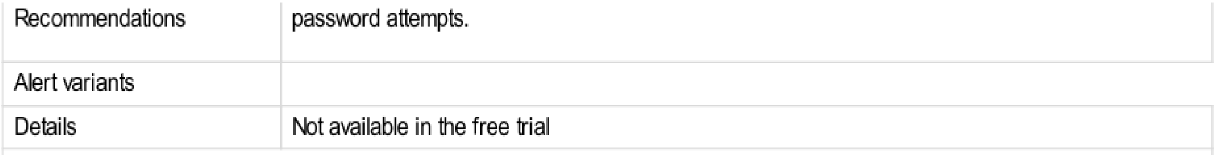
2. WordPress XML-RPC authentication brute force:



Web Server	
Alert group	**WordPress XML-RPC authentication brute force**
Severity	Medium
Description	WordPress provides an XML-RPC interface via the xmlrpc.php script. XML-RPC is remote procedure calling using HTTP as the transport and XML as the encoding. An attacker can abuse this interface to brute force authentication credentials using API calls such as **wp.getUsersBlogs**.
Recommendations	It is possible to disable the XML-RPC script if you do not want to use it. Consult references for a WordPress plugin that does that. If you don't want to disable XML-RPC you can monitor for XML-RPC authentication failures with a Web Application Firewall like ModSecurity.
Alert variants	
Details	Not available in the free trial

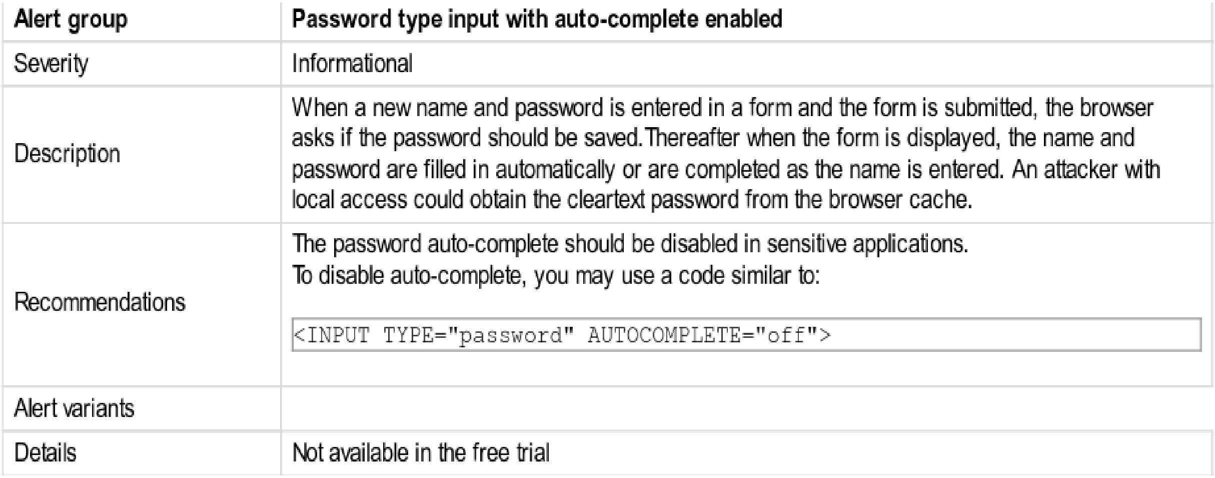
3. Login page password-guessing attack





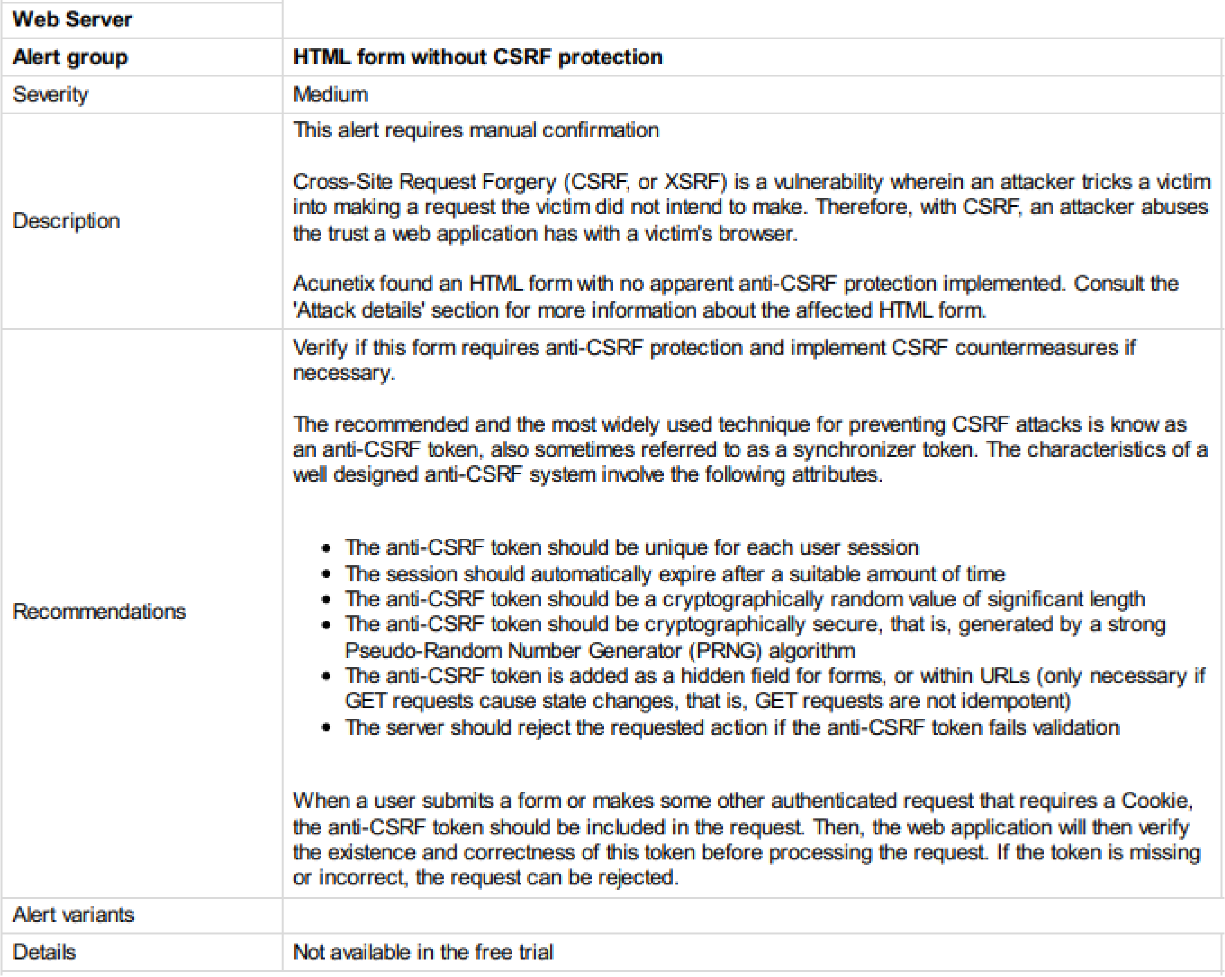
Web Server	
Alert group	**Login page password-guessing attack**
Severity	Low
Description	A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
Recommendations	It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.
Alert variants	
Details	Not available in the free trial

4.Password type input with auto-complete enabled



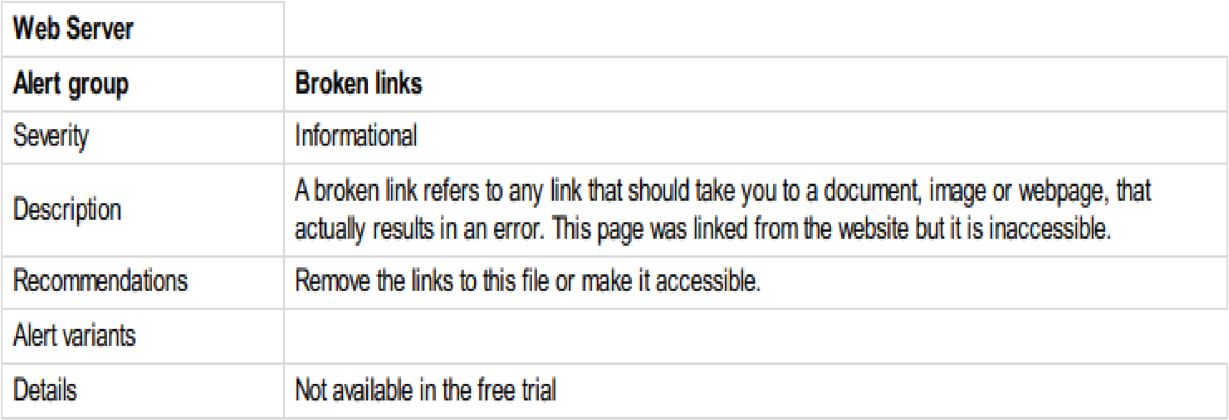
Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial

5.HTML form without CSRF protection:



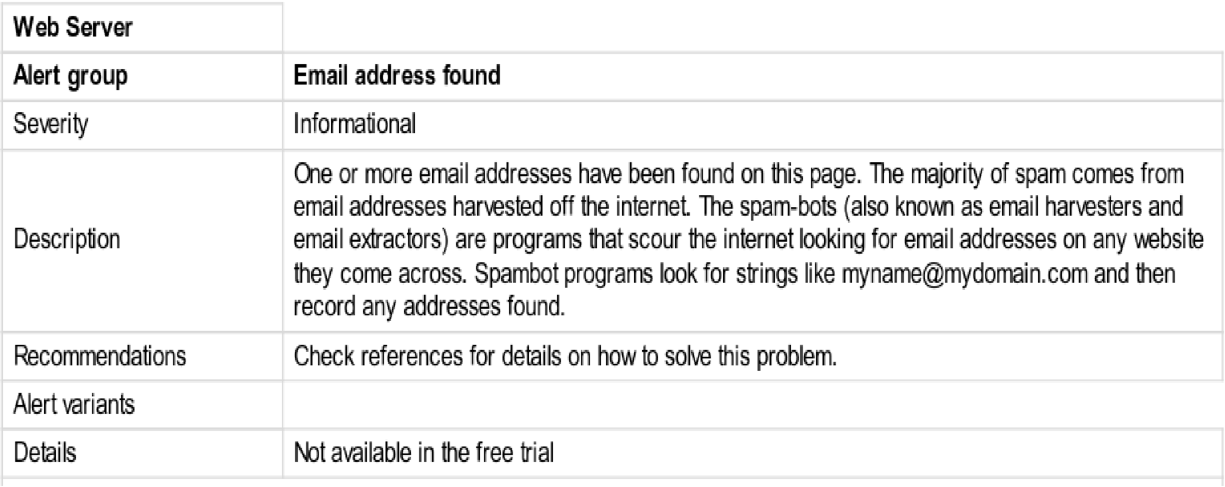
Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Not available in the free trial

6.Broken links:



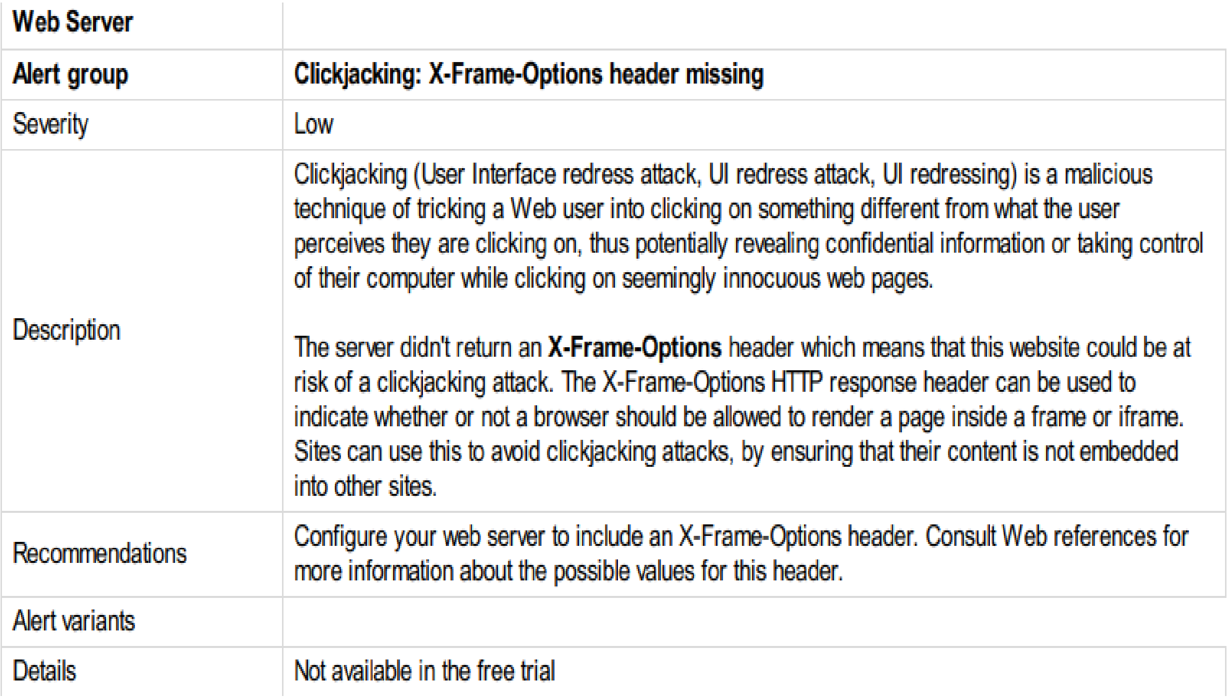
Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial

7. Email address found



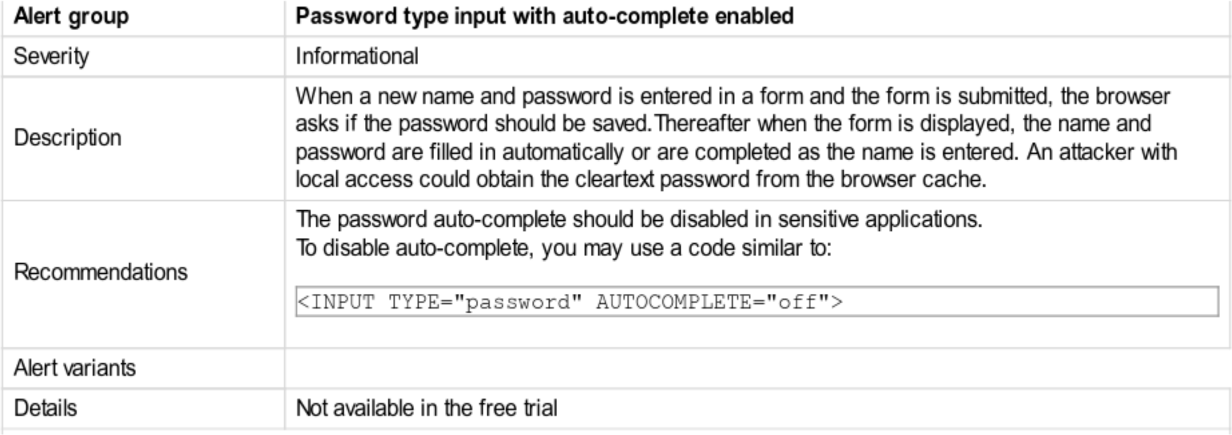
Web Server	
Alert group	**Email address found**
Severity	Informational
Description	One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Not available in the free trial

8.Clickjacking: X-Frame-Options header missing



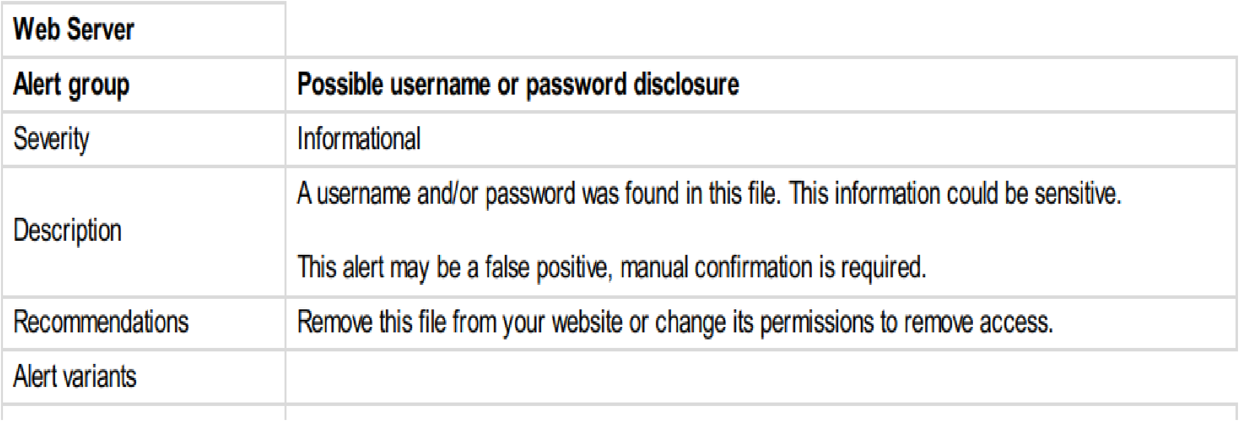
Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low
Description	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Recommendations	Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	Not available in the free trial

9.Password type input with auto-complete enabled



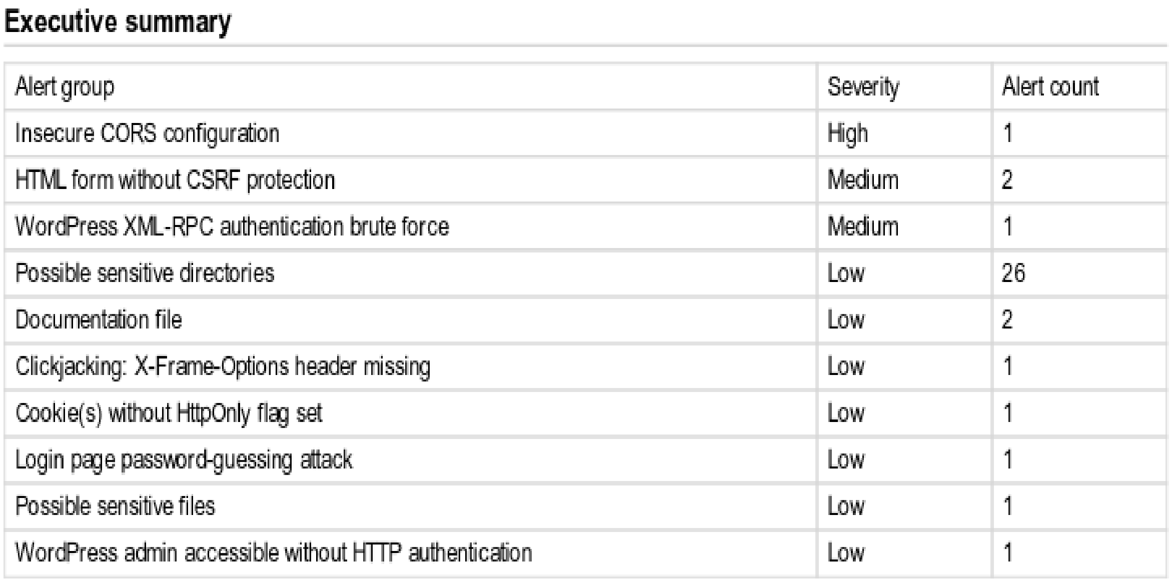
Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial

10.Possible username or password disclosure:



Web Server	
Alert group	**Possible username or password disclosure**
Severity	Informational
Description	A username and/or password was found in this file. This information could be sensitive. This alert may be a false positive, manual confirmation is required.
Recommendations	Remove this file from your website or change its permissions to remove access.
Alert variants	

Executing Summary Report :



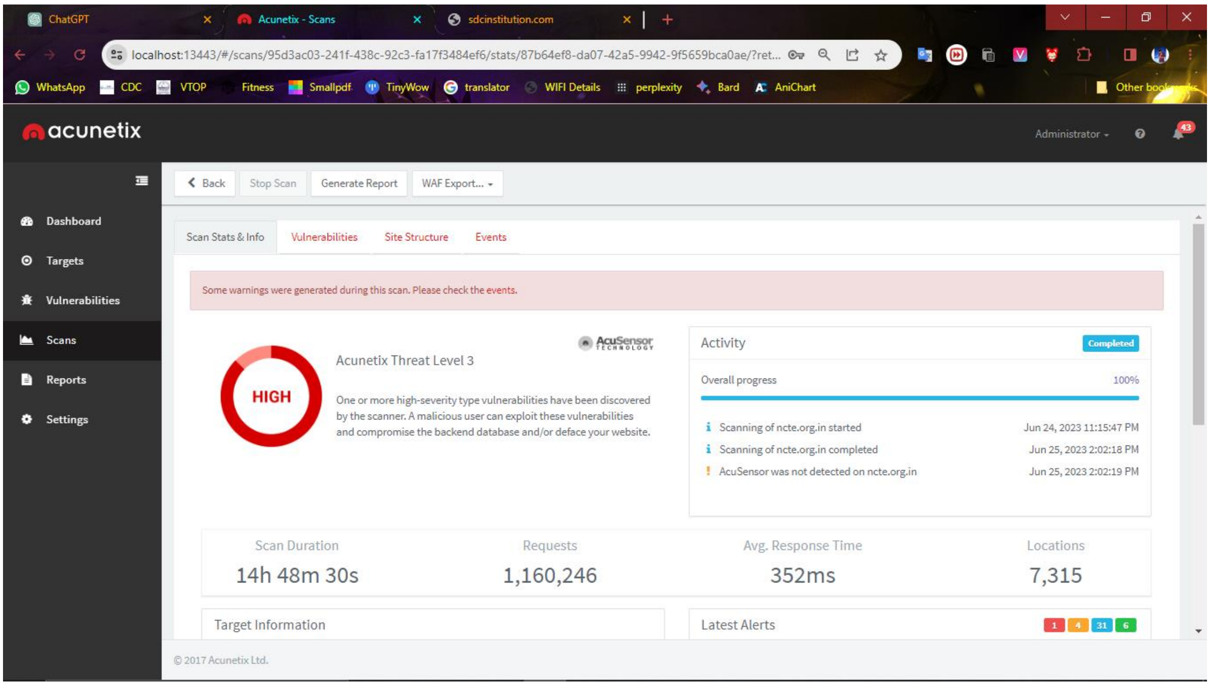
Executive summary

Alert group	Severity	Alert count
Insecure CORS configuration	High	1
HTML form without CSRF protection	Medium	2
WordPress XML-RPC authentication brute force	Medium	1
Possible sensitive directories	Low	26
Documentation file	Low	2
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Login page password-guessing attack	Low	1
Possible sensitive files	Low	1
WordPress admin accessible without HTTP authentication	Low	1

Practice Website: http://www.ncte.org.in/

Scanning Tool : Acunetix

<u>Scanning Details</u> :



Some warnings were generated during this scan. Please check the events.

Acunetix Threat Level 3

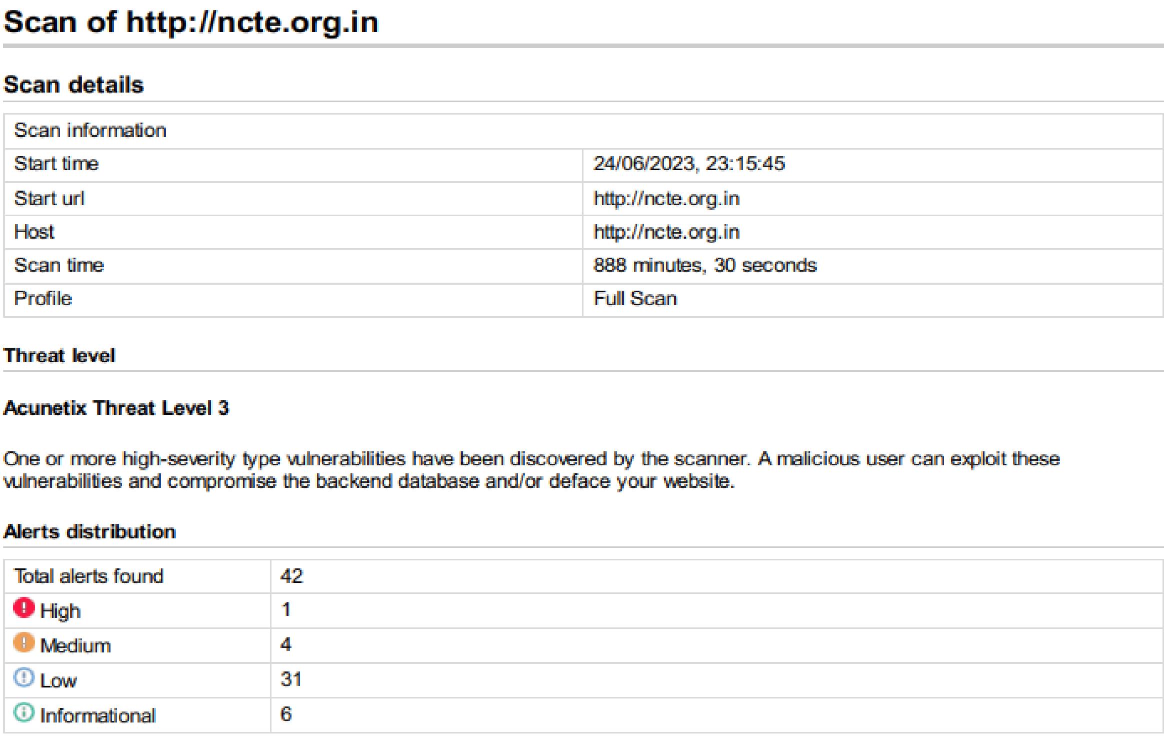
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Activity

Overall progress 100%

- Scanning of ncte.org.in started Jun 24, 2023 11:15:47 PM
- Scanning of ncte.org.in completed Jun 25, 2023 2:02:18 PM
- AcuSensor was not detected on ncte.org.in Jun 25, 2023 2:02:19 PM

Scan Duration	Requests	Avg. Response Time	Locations
14h 48m 30s	1,160,246	352ms	7,315



Scan of http://ncte.org.in

Scan details

Scan information	
Start time	24/06/2023, 23:15:45
Start url	http://ncte.org.in
Host	http://ncte.org.in
Scan time	888 minutes, 30 seconds
Profile	Full Scan

Threat level

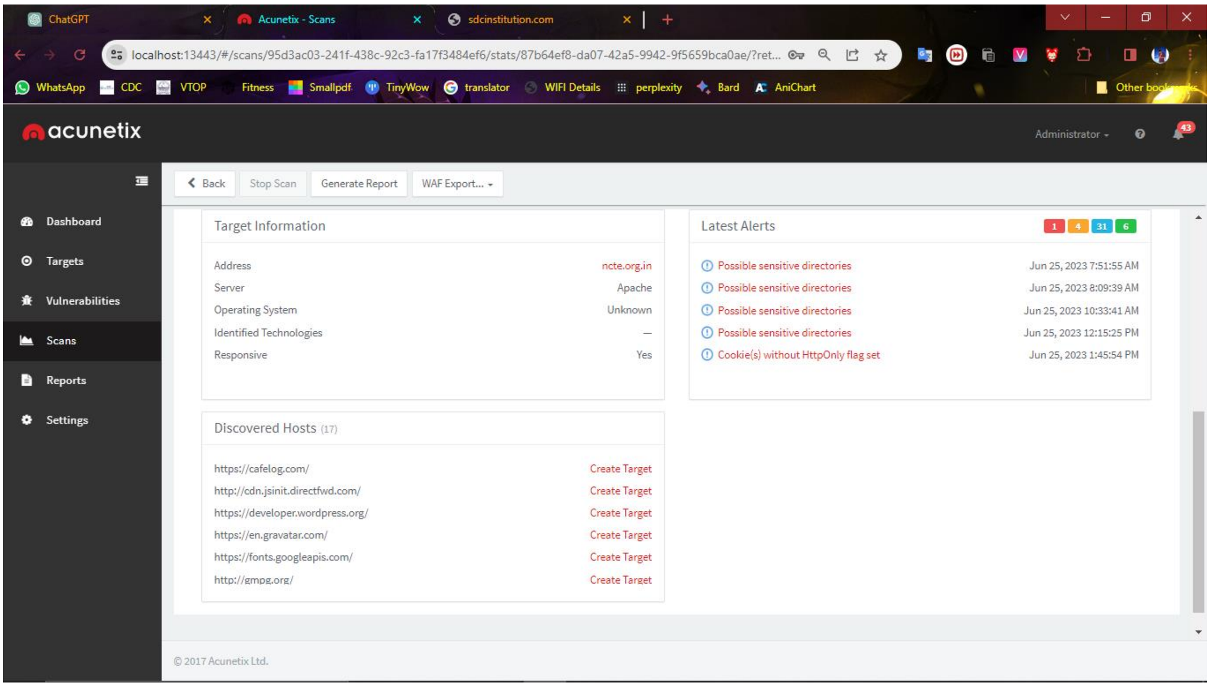
Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	42
High	1
Medium	4
Low	31
Informational	6

Target Information:



localhost:13443/#/scans/95d3ac03-241f-438c-92c3-fa17f3484ef6/stats/87b64ef8-da07-42a5-9942-9f5659bca0ae/?ret...

Target Information

Address	ncte.org.in
Server	Apache
Operating System	Unknown
Identified Technologies	—
Responsive	Yes

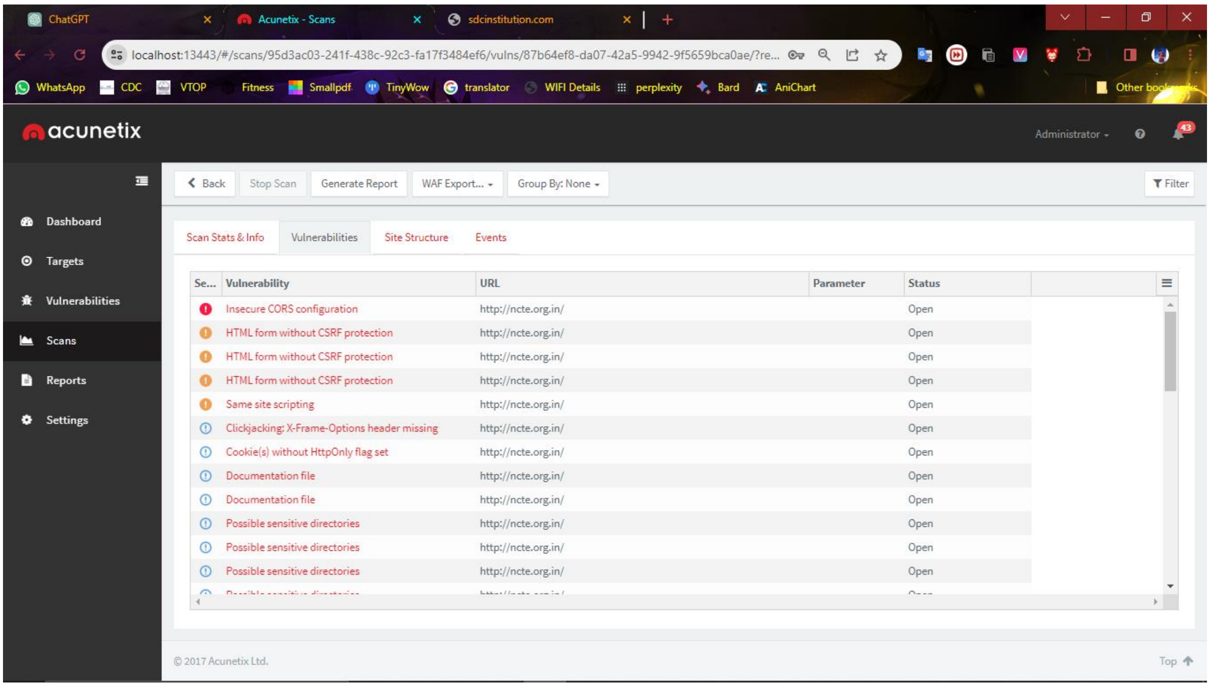
Latest Alerts 1 4 31 6

ⓘ Possible sensitive directories	Jun 25, 2023 7:51:55 AM
ⓘ Possible sensitive directories	Jun 25, 2023 8:09:39 AM
ⓘ Possible sensitive directories	Jun 25, 2023 10:33:41 AM
ⓘ Possible sensitive directories	Jun 25, 2023 12:15:25 PM
ⓘ Cookie(s) without HttpOnly flag set	Jun 25, 2023 1:45:54 PM

Discovered Hosts (17)

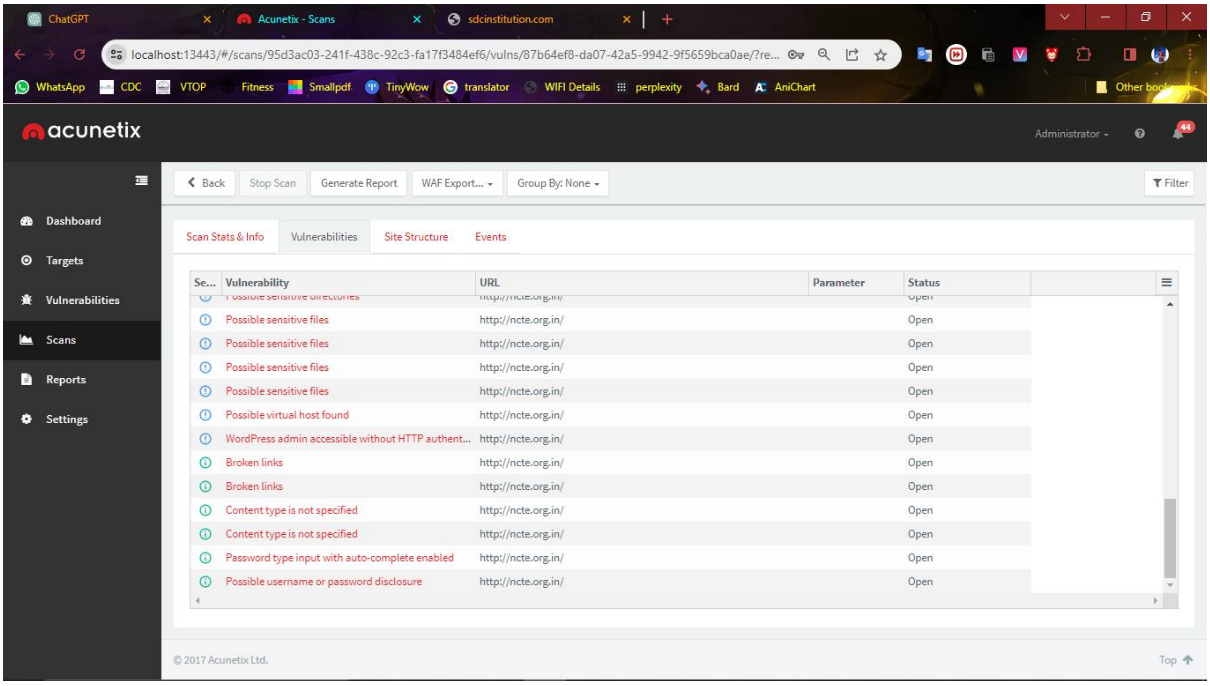
https://cafelog.com/	Create Target
http://cdn.jsinit.directfwd.com/	Create Target
https://developer.wordpress.org/	Create Target
https://en.gravatar.com/	Create Target
https://fonts.googleapis.com/	Create Target
http://gmpg.org/	Create Target

Available Vulnerabilities:



localhost:13443/#/scans/95d3ac03-241f-438c-92c3-fa17f3484ef6/vulns/87b64ef8-da07-42a5-9942-9f5659bca0ae/?re...

Se...	Vulnerability	URL	Parameter	Status
●	Insecure CORS configuration	http://ncte.org.in/		Open
●	HTML form without CSRF protection	http://ncte.org.in/		Open
●	HTML form without CSRF protection	http://ncte.org.in/		Open
●	HTML form without CSRF protection	http://ncte.org.in/		Open
●	Same site scripting	http://ncte.org.in/		Open
ⓘ	Clickjacking: X-Frame-Options header missing	http://ncte.org.in/		Open
ⓘ	Cookie(s) without HttpOnly flag set	http://ncte.org.in/		Open
ⓘ	Documentation file	http://ncte.org.in/		Open
ⓘ	Documentation file	http://ncte.org.in/		Open
ⓘ	Possible sensitive directories	http://ncte.org.in/		Open
ⓘ	Possible sensitive directories	http://ncte.org.in/		Open
ⓘ	Possible sensitive directories	http://ncte.org.in/		Open
ⓘ	Possible sensitive directories	http://ncte.org.in/		Open



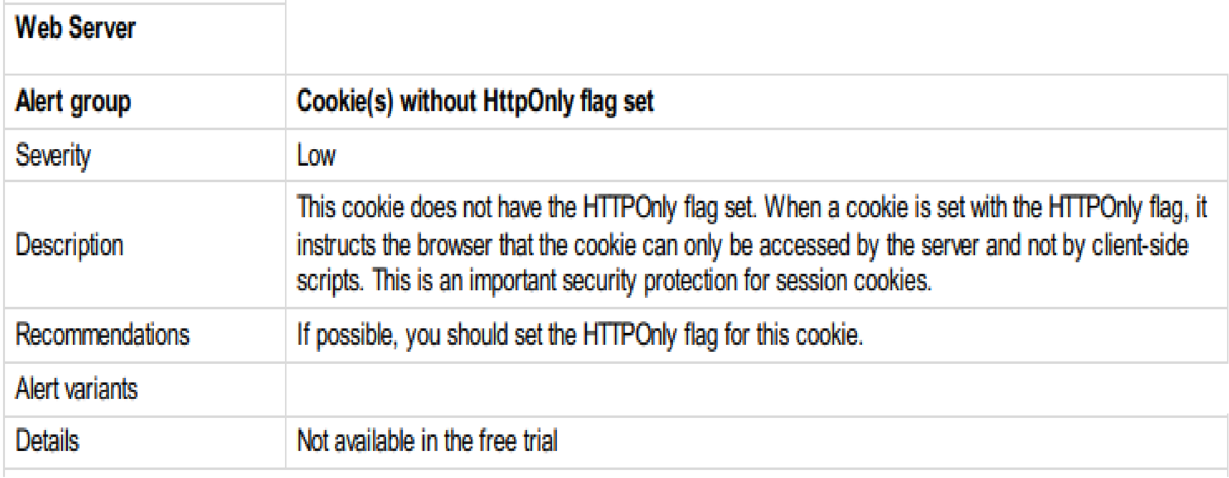
Se...	Vulnerability	URL	Parameter	Status
ⓘ	Possible sensitive directories	http://ncte.org.in/		Open
ⓘ	Possible sensitive files	http://ncte.org.in/		Open
ⓘ	Possible sensitive files	http://ncte.org.in/		Open
ⓘ	Possible sensitive files	http://ncte.org.in/		Open
ⓘ	Possible sensitive files	http://ncte.org.in/		Open
ⓘ	Possible virtual host found	http://ncte.org.in/		Open
ⓘ	WordPress admin accessible without HTTP authent...	http://ncte.org.in/		Open
ⓘ	Broken links	http://ncte.org.in/		Open
ⓘ	Broken links	http://ncte.org.in/		Open
ⓘ	Content type is not specified	http://ncte.org.in/		Open
ⓘ	Content type is not specified	http://ncte.org.in/		Open
ⓘ	Password type input with auto-complete enabled	http://ncte.org.in/		Open
ⓘ	Possible username or password disclosure	http://ncte.org.in/		Open

Vulnerbility Details :

1.Insecure CORS configuration

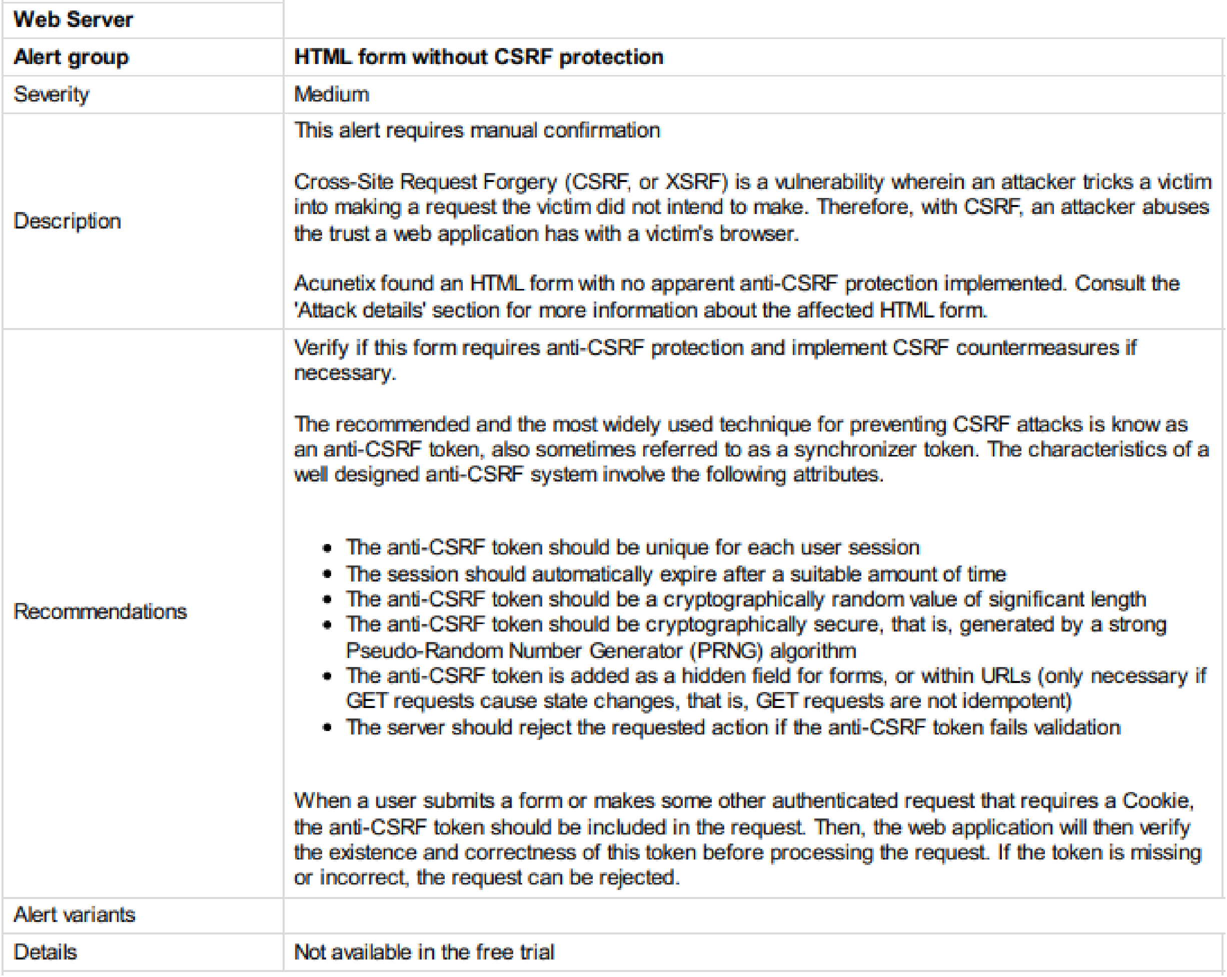
Web Server	
Alert group	**Insecure CORS configuration**
Severity	High
Description	CORS (Cross-Origin Resource Sharing) defines a mechanism to enable client-side cross-origin requests. This application is using CORS in an insecure way. The web application returns the following headers: • **Access-Control-Allow-Credentials: true** • **Access-Control-Allow-Origin: copy of the Origin header from request** In this configuration any website can issue requests made with **user credentials** and read the responses to these requests.
Recommendations	Allow only selected, trusted domains in the Access-Control-Allow-Origin header.
Alert variants	
Details	Not available in the free trial

2.Cookie(s) without HttpOnly flag set :



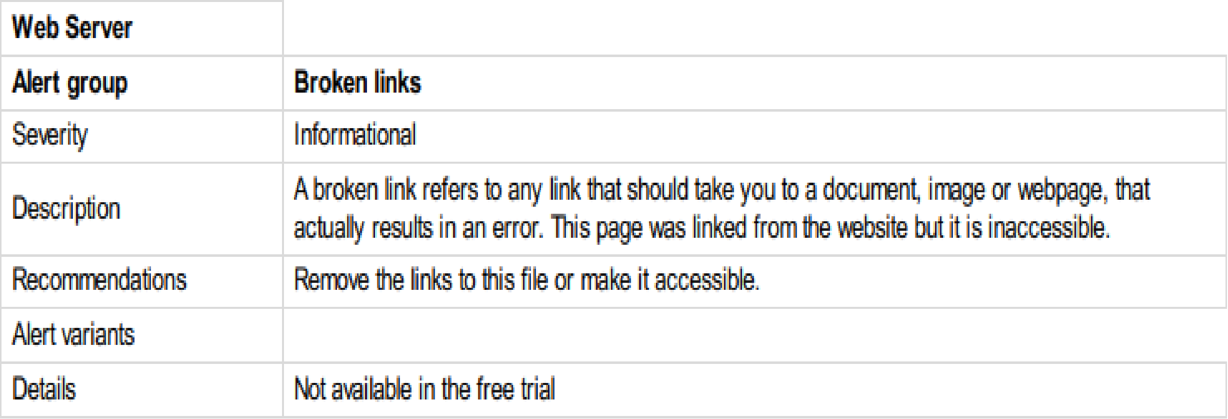
Web Server	
Alert group	**Cookie(s) without HttpOnly flag set**
Severity	Low
Description	This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HTTPOnly flag for this cookie.
Alert variants	
Details	Not available in the free trial

3.HTML form without CSRF protection:



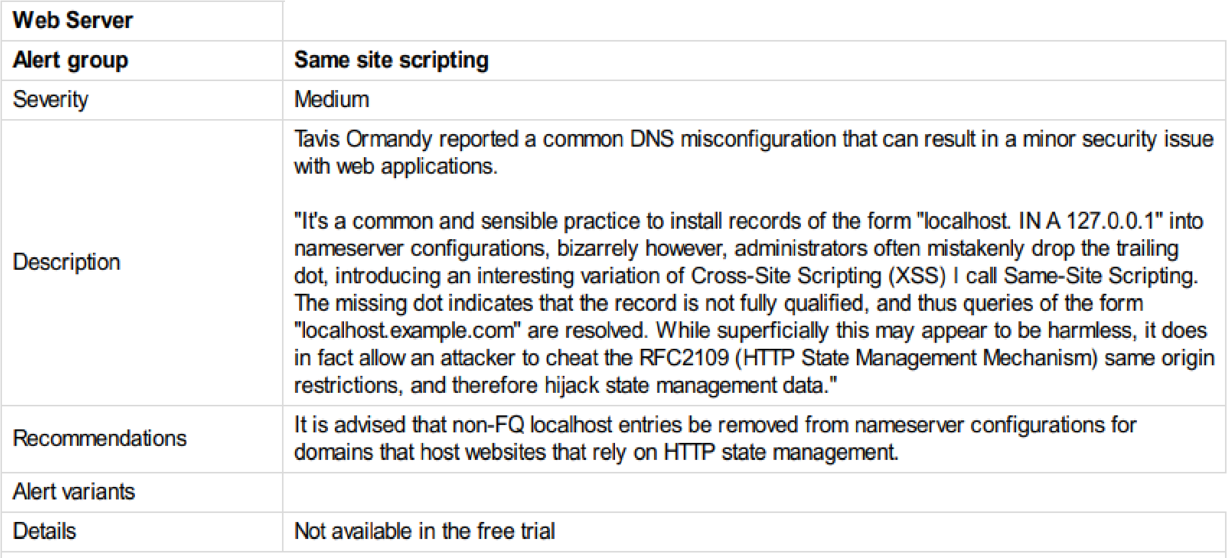
Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Not available in the free trial

4.Broken links:



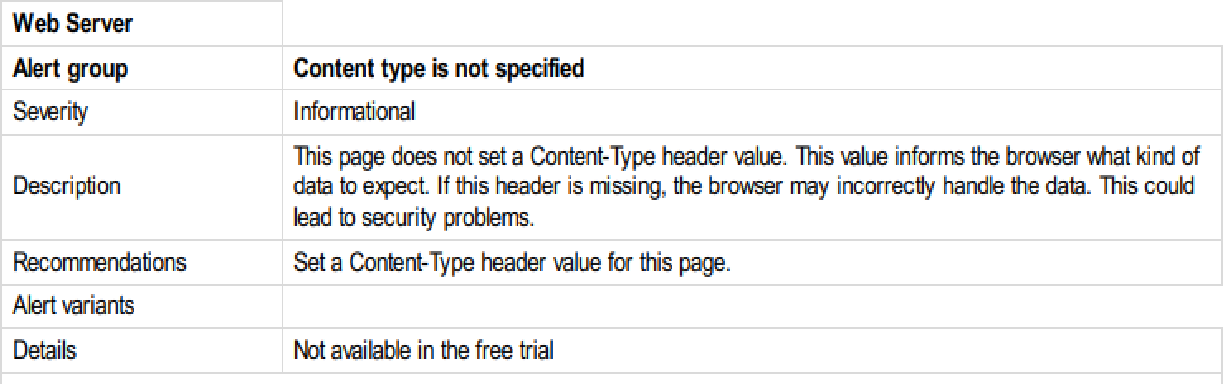
Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial

5.Same site scripting:



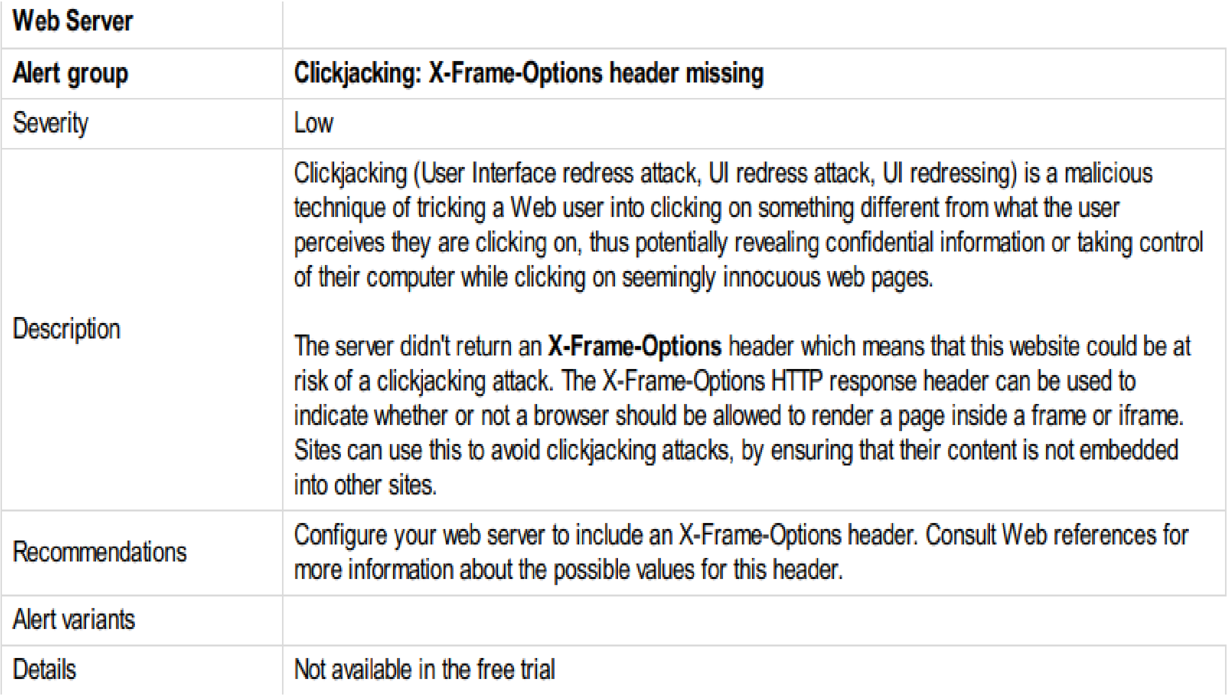
Web Server	
Alert group	**Same site scripting**
Severity	Medium
Description	Tavis Ormandy reported a common DNS misconfiguration that can result in a minor security issue with web applications. "It's a common and sensible practice to install records of the form "localhost. IN A 127.0.0.1" into nameserver configurations, bizarrely however, administrators often mistakenly drop the trailing dot, introducing an interesting variation of Cross-Site Scripting (XSS) I call Same-Site Scripting. The missing dot indicates that the record is not fully qualified, and thus queries of the form "localhost.example.com" are resolved. While superficially this may appear to be harmless, it does in fact allow an attacker to cheat the RFC2109 (HTTP State Management Mechanism) same origin restrictions, and therefore hijack state management data."
Recommendations	It is advised that non-FQ localhost entries be removed from nameserver configurations for domains that host websites that rely on HTTP state management.
Alert variants	
Details	Not available in the free trial

6.Content type is not specified:



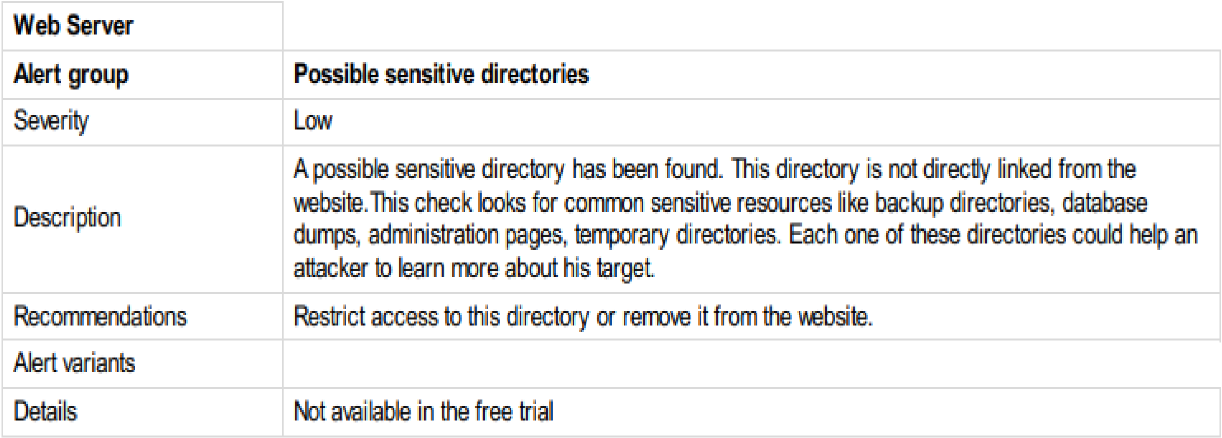
Web Server	
Alert group	**Content type is not specified**
Severity	Informational
Description	This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.
Recommendations	Set a Content-Type header value for this page.
Alert variants	
Details	Not available in the free trial

7.Clickjacking: X-Frame-Options header missing



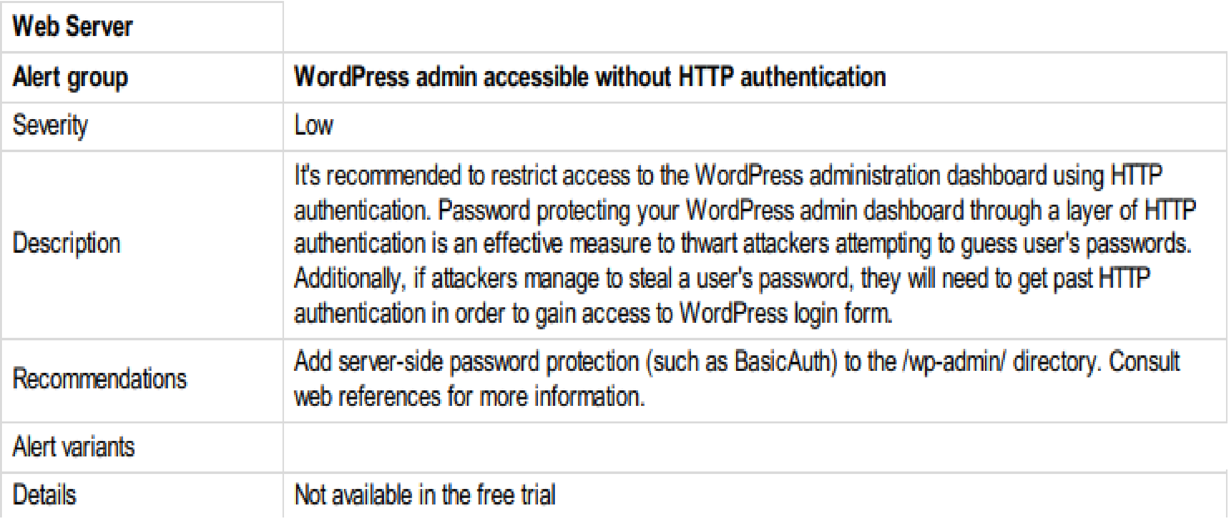
Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low
Description	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Recommendations	Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	Not available in the free trial

8.Possible sensitive directories :



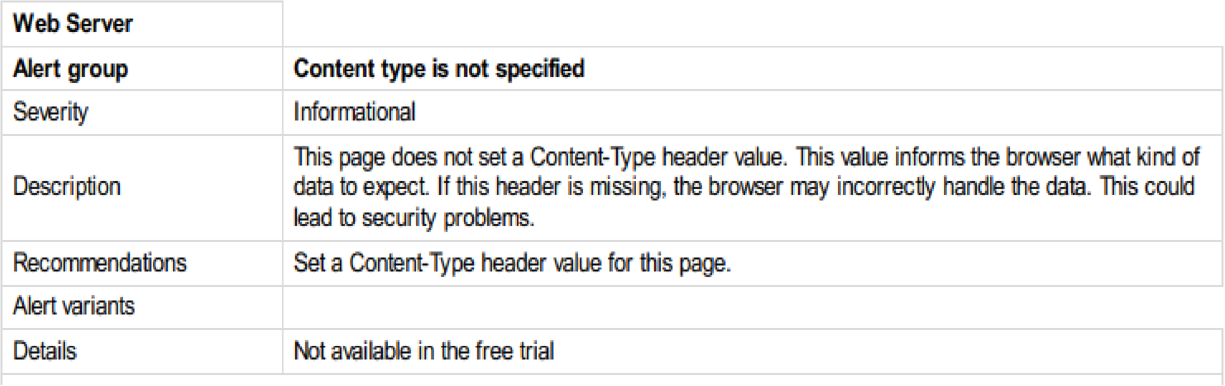
Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to this directory or remove it from the website.
Alert variants	
Details	Not available in the free trial

9.WordPress admin accessible without HTTP authentication:



Web Server	
Alert group	**WordPress admin accessible without HTTP authentication**
Severity	Low
Description	It's recommended to restrict access to the WordPress administration dashboard using HTTP authentication. Password protecting your WordPress admin dashboard through a layer of HTTP authentication is an effective measure to thwart attackers attempting to guess user's passwords. Additionally, if attackers manage to steal a user's password, they will need to get past HTTP authentication in order to gain access to WordPress login form.
Recommendations	Add server-side password protection (such as BasicAuth) to the /wp-admin/ directory. Consult web references for more information.
Alert variants	
Details	Not available in the free trial

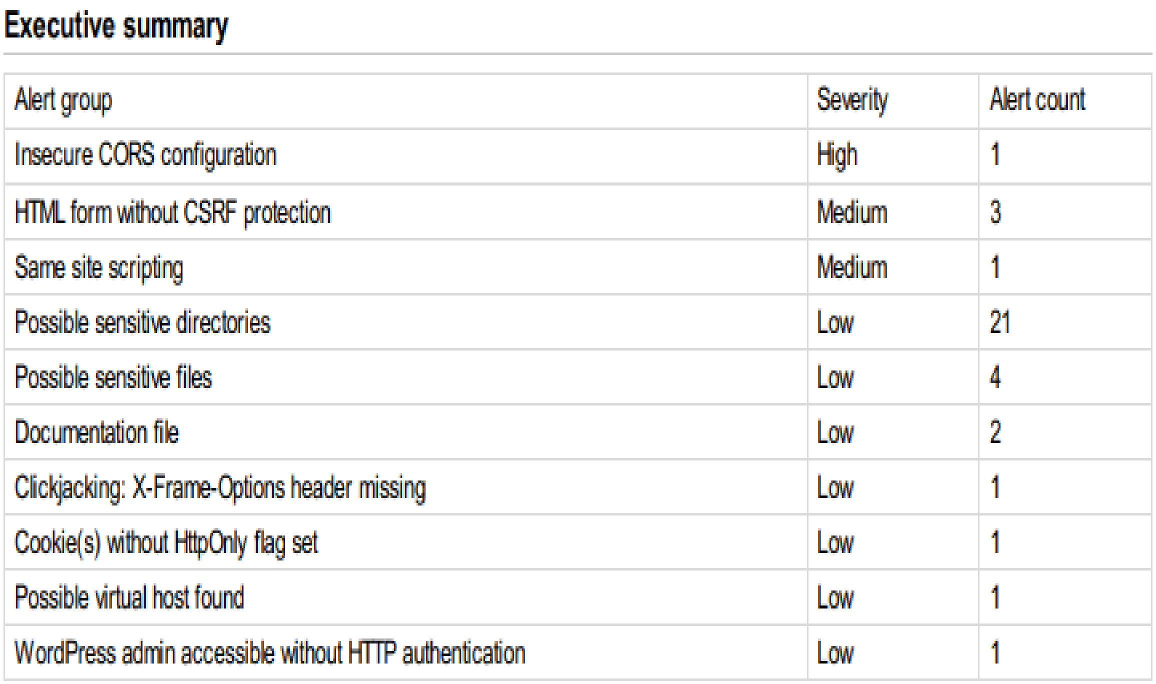
10.Content type is not specified:



Web Server	
Alert group	**Content type is not specified**
Severity	Informational
Description	This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.
Recommendations	Set a Content-Type header value for this page.
Alert variants	
Details	Not available in the free trial

+

Executing Summary Report :



Executive summary

Alert group	Severity	Alert count
Insecure CORS configuration	High	1
HTML form without CSRF protection	Medium	3
Same site scripting	Medium	1
Possible sensitive directories	Low	21
Possible sensitive files	Low	4
Documentation file	Low	2
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Possible virtual host found	Low	1
WordPress admin accessible without HTTP authentication	Low	1