

Affected Items Report

Acunetix Security Audit

11 May 2019

Scan of www.frc.utn.edu.ar

Scan details



Scan information	
Start time	11/05/2019, 14:06:25
Start url	https://www.frc.utn.edu.ar/
Host	www.frc.utn.edu.ar
Scan time	60 minutes, 18 seconds
Profile	Full Scan
Server information	Microsoft-IIS/6.0
Responsive	True
Server OS	Windows
Server technologies	ASP

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	38
 High	1
 Medium	11
 Low	14
 Informational	12

Affected items

Web Server	
Alert group	Cross site scripting (verified)
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	Application error message
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>Application error or warning messages may expose sensitive information about an application's internal workings to an attacker.</p> <p>Acunetix found an error or warning message that may disclose sensitive information. The message may also contain the location of the file that produced an unhandled exception. Consult the 'Attack details' section for more information about the affected page.</p>
Recommendations	Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>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.</p> <p>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.</p>

Recommendations	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>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.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>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.</p> <p>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.</p>
Recommendations	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>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.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>

Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>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.</p> <p>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.</p>
Recommendations	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>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.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>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.</p> <p>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.</p>

Recommendations	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>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.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>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.</p> <p>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.</p>
Recommendations	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>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.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>

Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>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.</p> <p>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.</p>
Recommendations	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>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.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>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.</p> <p>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.</p>

Recommendations	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>The recommended and the most widely used technique for preventing CSRF attacks is known 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.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	HTML form without CSRF protection
Severity	Medium
Description	<p>This alert requires manual confirmation</p> <p>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.</p> <p>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.</p>
Recommendations	<p>Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary.</p> <p>The recommended and the most widely used technique for preventing CSRF attacks is known 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.</p> <ul style="list-style-type: none"> • 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 <p>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.</p>

Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	TLS 1.0 enabled
Severity	Medium
Description	The web server supports encryption through TLS 1.0. TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.
Recommendations	It is recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	Vulnerable Javascript library
Severity	Medium
Description	You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.
Recommendations	Upgrade to the latest version.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	Clickjacking: X-Frame-Options header missing
Severity	Low
Description	<p>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.</p> <p>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.</p>
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
Not available in the free trial	

Web Server	
Alert group	Insecure Flash embed parameter
Severity	Low

Description	<p>The AllowScriptAccess parameter in the HTML code that loads a SWF file controls the ability to perform outbound URL access from within the SWF file. Set this parameter inside the PARAM or EMBED tag. If no value is set for AllowScriptAccess, the SWF file and the HTML page can communicate only if both are from the same domain.</p> <p>This HTML page embeds a SWF file with AllowScriptAccess parameter set to "always". When AllowScriptAccess is "always," the SWF file can communicate with the HTML page in which it is embedded. This rule applies even when the SWF file is from a different domain than the HTML page. This represents a security issue and can result in attacks such as script injection and cross-domain privilege escalation.</p>
Recommendations	Set AllowScriptAccess to 'never' or remove the AllowScriptAccess parameter.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	Login page password-guessing attack
Severity	Low
Description	<p>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.</p> <p>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.</p>
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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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

Not available in the free trial	
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
Not available in the free trial	

Web Server	
Alert group	Content Security Policy (CSP) not implemented
Severity	Informational
Description	<p>Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.</p> <p>Content Security Policy (CSP) can be implemented by adding a Content-Security-Policy header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:</p> <div><pre>Content-Security-Policy: default-src 'self'; script-src 'self' https://code.jquery.com;</pre></div> <p>It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.</p>
Recommendations	It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

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
Not available in the free trial	

Web Server	
Alert group	Microsoft IIS version disclosure
Severity	Informational
Description	The HTTP responses returned by this web application include a header named Server . The value of this header includes the version of Microsoft IIS server.
Recommendations	Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult web references for more information.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
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	<div>The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to:</div> <div><INPUT TYPE="password" AUTOCOMPLETE="off"></div>
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	Subresource Integrity (SRI) not implemented
Severity	Informational
Description	<div>Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.</div> <div>Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha265, sha384 or sha512.</div> <div>The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.</div>
Recommendations	<div>Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).</div> <div>For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.</div> <div><script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HN crossorigin="anonymous"></script></div>
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Web Server	
Alert group	TLS 1.1 enabled
Severity	Informational

Description	The web server supports encryption through TLS 1.1. When aiming for Payment Card Industry (PCI) Data Security Standard (DSS) compliance, it is recommended (although at the time of writing not required) to use TLS 1.2 or higher instead. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.
Recommendations	It is recommended to disable TLS 1.1 and replace it with TLS 1.2 or higher.
Alert variants	
Details	Not available in the free trial
Not available in the free trial	

Scanned items (coverage report)

<https://www.frc.utn.edu.ar/>

<https://www.frc.utn.edu.ar/admin/>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/imagenes/>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/nivo-slider/>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/nivo-slider/jquery-1.6.1.min.js>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/nivo-slider/jquery.nivo.slider.pack.js>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/nivo-slider/nivo-slider.css>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/nivo-slider/style.css>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/tooltip/>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/tooltip/jquery.tools.min.js>

<https://www.frc.utn.edu.ar/autogestion-aniversario-10/tooltip/style.css>

<https://www.frc.utn.edu.ar/autogestion4/>

<https://www.frc.utn.edu.ar/autogestion4/front.css>

<https://www.frc.utn.edu.ar/autogestion4/images/>

<https://www.frc.utn.edu.ar/autogestion4/jquery-ui-1.8.16.custom.min.js>

<https://www.frc.utn.edu.ar/autogestion4/jquery.form.js>

<https://www.frc.utn.edu.ar/autogestion4/priorizar.frc>

<https://www.frc.utn.edu.ar/autogestion4/twitmarquee.js>

<https://www.frc.utn.edu.ar/ayuda/>

<https://www.frc.utn.edu.ar/ayuda/default.frc>

<https://www.frc.utn.edu.ar/ayuda/imagenes/>

<https://www.frc.utn.edu.ar/ayuda/wap/>

<https://www.frc.utn.edu.ar/biblioteca/>

<https://www.frc.utn.edu.ar/biblioteca/busqueda.asp>

<https://www.frc.utn.edu.ar/biblioteca/busqueda.js>

<https://www.frc.utn.edu.ar/biblioteca/imagenes/>

<https://www.frc.utn.edu.ar/biblioteca/index.htm>

<https://www.frc.utn.edu.ar/bibliotecaCentral/>

<https://www.frc.utn.edu.ar/bibliotecaCentral/Busqueda.asp>

<https://www.frc.utn.edu.ar/bibliotecaCentral/Contactenos.htm>

<https://www.frc.utn.edu.ar/bibliotecaCentral/imagenes/>

<https://www.frc.utn.edu.ar/bibliotecaCentral/index.htm>

<https://www.frc.utn.edu.ar/bibliotecaCentral/Informacion-General.htm>

<https://www.frc.utn.edu.ar/bibliotecaCentral/Links.htm>

<https://www.frc.utn.edu.ar/bibliotecaCentral/Mision-Objetivos.htm>

<https://www.frc.utn.edu.ar/bibliotecacentral/nueva/>

<https://www.frc.utn.edu.ar/bibliotecaCentral/Reglamento.htm>

<https://www.frc.utn.edu.ar/bibliotecaCentral/Servicios.htm>

<https://www.frc.utn.edu.ar/computos/>

<https://www.frc.utn.edu.ar/computos/admin/>

<https://www.frc.utn.edu.ar/computos/apps/>

<https://www.frc.utn.edu.ar/computos/img/>

<https://www.frc.utn.edu.ar/computos/js/>

<https://www.frc.utn.edu.ar/computos/pub/>

<https://www.frc.utn.edu.ar/computos/pub/image/>

<https://www.frc.utn.edu.ar/computos/pub/image/eduroam/>

<https://www.frc.utn.edu.ar/computos/rss/>

<https://www.frc.utn.edu.ar/default.frc>

<https://www.frc.utn.edu.ar/dispensador.frc>

<https://www.frc.utn.edu.ar/elecciones/>

<https://www.frc.utn.edu.ar/elecciones/dasuten/>

<https://www.frc.utn.edu.ar/encuestas/>

<https://www.frc.utn.edu.ar/encuestas/censo/>

<https://www.frc.utn.edu.ar/estilos/>

<https://www.frc.utn.edu.ar/estilos/ppal.css>

<https://www.frc.utn.edu.ar/funciones/>

<https://www.frc.utn.edu.ar/funciones/contador.frc>

<https://www.frc.utn.edu.ar/g/>

<https://www.frc.utn.edu.ar/g/banner/>

<https://www.frc.utn.edu.ar/g/file/>

<https://www.frc.utn.edu.ar/g/flash/>
<https://www.frc.utn.edu.ar/g/image/>
<https://www.frc.utn.edu.ar/imagenes/>
<https://www.frc.utn.edu.ar/imagenes/banner/>
<https://www.frc.utn.edu.ar/imagenes/navidad/>
<https://www.frc.utn.edu.ar/imagenes/otros/>
<https://www.frc.utn.edu.ar/ingresantes/>
<https://www.frc.utn.edu.ar/ingresantes/apps/>
<https://www.frc.utn.edu.ar/ingresantes/img/>
<https://www.frc.utn.edu.ar/ingresantes/js/>
<https://www.frc.utn.edu.ar/ingresantes/pub/>
<https://www.frc.utn.edu.ar/ingresantes/pub/file/>
<https://www.frc.utn.edu.ar/ingresantes/pub/image/>
<https://www.frc.utn.edu.ar/ingresantes/rss/>
<https://www.frc.utn.edu.ar/institucional/>
<https://www.frc.utn.edu.ar/institucional/telefonos.frc>
<https://www.frc.utn.edu.ar/logon.frc>
<https://www.frc.utn.edu.ar/portal/>
<https://www.frc.utn.edu.ar/portal/apps/>
<https://www.frc.utn.edu.ar/portal/img/>
<https://www.frc.utn.edu.ar/portal/js/>
<https://www.frc.utn.edu.ar/portal/rss/>
<https://www.frc.utn.edu.ar/prensa/>
<https://www.frc.utn.edu.ar/prensa/apps/>
<https://www.frc.utn.edu.ar/prensa/default.frc>
<https://www.frc.utn.edu.ar/prensa/img/>
<https://www.frc.utn.edu.ar/prensa/js/>
<https://www.frc.utn.edu.ar/prensa/pub/>
<https://www.frc.utn.edu.ar/prensa/pub/file/>
<https://www.frc.utn.edu.ar/prensa/pub/file/2018/>
<https://www.frc.utn.edu.ar/prensa/pub/file/2019/>
<https://www.frc.utn.edu.ar/prensa/pub/image/>
<https://www.frc.utn.edu.ar/prensa/pub/image/2017/>
<https://www.frc.utn.edu.ar/prensa/pub/image/2018/>
<https://www.frc.utn.edu.ar/prensa/pub/image/2019/>
<https://www.frc.utn.edu.ar/prensa/pub/image/Banner/>
<https://www.frc.utn.edu.ar/prensa/pub/image/Prensa/>
<https://www.frc.utn.edu.ar/prensa/rss/>
<https://www.frc.utn.edu.ar/radio/>
<https://www.frc.utn.edu.ar/radio/apps/>
<https://www.frc.utn.edu.ar/radio/img/>
<https://www.frc.utn.edu.ar/radio/js/>
<https://www.frc.utn.edu.ar/radio/pub/>
<https://www.frc.utn.edu.ar/radio/pub/image/>
<https://www.frc.utn.edu.ar/radio/rss/>
<https://www.frc.utn.edu.ar/scripts/>
<https://www.frc.utn.edu.ar/scripts/app/>
<https://www.frc.utn.edu.ar/scripts/app/sugerencias.frc>
<https://www.frc.utn.edu.ar/scripts/cycle/>
<https://www.frc.utn.edu.ar/scripts/cycle/jquery.cycle.lite.min.js>
<https://www.frc.utn.edu.ar/scripts/forms/>
<https://www.frc.utn.edu.ar/scripts/forms/jquery.form.pck.js>
<https://www.frc.utn.edu.ar/scripts/frc/>
<https://www.frc.utn.edu.ar/scripts/frc/ppal.js>
<https://www.frc.utn.edu.ar/scripts/hoverIntent/>
<https://www.frc.utn.edu.ar/scripts/hoverIntent/jquery.hoverIntent.js>
<https://www.frc.utn.edu.ar/scripts/jqueryCore/>
<https://www.frc.utn.edu.ar/scripts/jqueryCore/jquery.js>
<https://www.frc.utn.edu.ar/scripts/ssubnav/>
<https://www.frc.utn.edu.ar/scripts/ssubnav/ssubnav.css>
<https://www.frc.utn.edu.ar/scripts/ssubnav/ssubnav.js>
<https://www.frc.utn.edu.ar/scripts/validate/>
<https://www.frc.utn.edu.ar/scripts/validate/jquery.validate.pck.js>
<https://www.frc.utn.edu.ar/secretarias/>

<https://www.frc.utn.edu.ar/secretarias/academica/>
<https://www.frc.utn.edu.ar/secretarias/academica/carreras/>
<https://www.frc.utn.edu.ar/secretarias/riyrsu/>
<https://www.frc.utn.edu.ar/secretarias/scyt/>
<https://www.frc.utn.edu.ar/share/>
<https://www.frc.utn.edu.ar/sitemap.xml>
<https://www.frc.utn.edu.ar/Skins/>
<https://www.frc.utn.edu.ar/Skins/admin/>
<https://www.frc.utn.edu.ar/Skins/plantillas/>
<https://www.frc.utn.edu.ar/Skins/plantillas/computos/>
<https://www.frc.utn.edu.ar/Skins/plantillas/computos/estilos/>
<https://www.frc.utn.edu.ar/Skins/plantillas/computos/estilos/principal.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/computos/estilos/principalImprimir.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/computos/estilos/tamano2.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/computos/imagenes/>
<https://www.frc.utn.edu.ar/Skins/plantillas/computos/imagenes/barra/>
<https://www.frc.utn.edu.ar/Skins/plantillas/Comunes/>
<https://www.frc.utn.edu.ar/Skins/plantillas/Comunes/js/>
<https://www.frc.utn.edu.ar/Skins/plantillas/Comunes/js/acciones.js>
<https://www.frc.utn.edu.ar/Skins/plantillas/Comunes/js/generales.js>
<https://www.frc.utn.edu.ar/Skins/plantillas/Comunes/js/stm31.js>
<https://www.frc.utn.edu.ar/Skins/plantillas/gral2007/>
<https://www.frc.utn.edu.ar/Skins/plantillas/gral2007/estilos/>
<https://www.frc.utn.edu.ar/Skins/plantillas/gral2007/estilos/autoico.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/gral2007/estilos/principal.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/gral2007/estilos/principalImprimir.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/gral2007/estilos/tamano2.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/gral2007/imagenes/>
<https://www.frc.utn.edu.ar/Skins/plantillas/prensa/>
<https://www.frc.utn.edu.ar/Skins/plantillas/prensa/estilos/>
<https://www.frc.utn.edu.ar/Skins/plantillas/prensa/estilos/principal.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/prensa/estilos/principalImprimir.css>
<https://www.frc.utn.edu.ar/Skins/plantillas/prensa/imagenes/>
<https://www.frc.utn.edu.ar/Skins/scripts/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/bgstretch/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/bgstretch/jquery.backstretch.min.js>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/core/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/core/jquery-1.10.2.min.js>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/dataTable/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/dataTable/media/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/dataTable/media/es.txt>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/dataTable/media/imagenes/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/dataTable/media/js/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/dataTable/media/js/jquery.dataTables.js>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/roundCorner/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/roundCorner/jquery.corner.js>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/showHide/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/showHide/jsh.css>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/showHide/jsh.js>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/toogleElements/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/toogleElements/jquery.toggleElements.pack.js>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/toogleElements/toggleElements.css>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/translate/>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/translate/jquery.sundaymorning.css>
<https://www.frc.utn.edu.ar/Skins/scripts/jquery/translate/jquery.sundaymorning.js>
<https://www.frc.utn.edu.ar/test/>
<https://www.frc.utn.edu.ar/tracker/>
<https://www.frc.utn.edu.ar/ws/>