Acunetix
by Invicti

Affected Items Report

Acunetix Security Audit

2026-02-10

Generated by Acunetix

Vulnerabilities

Scan details

Scan information	
Start url	http://10.67.253.121/
Host	http://10.67.253.121/

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	33
Critical	0
High	2
Medium	18
Low	7
Informational	6

Affected items

/core/config/	
Alert group	**Symfony databases.yml configuration file**
Severity	High
Description	A Symfony databases.yml configuration file (**config/databases.yml**) was found in this directory. The databases.yml configuration allows for the configuration of the database connection. This file may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.
Recommendations	Remove or restrict access to all configuration files acessible from internet.
Alert variants	

Details	Pattern found:
	
	`all:`
	`  doctrine:`
	`  class: sfDoctrineDatabase`
	`  param:`
	`  dsn: 'mysql:dbname=qdpm;host=localhost'`
	`  profiler: false`
	`  username: otis`
	`  password: "<?php echo urlencode('rush') ; ?>"`
	`  attributes:`
	`  quote_identifier: true`

```
GET /core/config/databases.yml HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**qdPM Information Disclosure**
Severity	High
Description	Due to a misconfiguration of a web server, qdPM configuration files are accessible for unauthenticated users
Recommendations	Restrict access to configuration files
Alert variants	
Details	

```
GET /core/config/databases.yml HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.
Recommendations	
Alert variants	
Details	bootstrap.js v3.0.3-3.0.3

Web Server	
Alert group	**Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.
Recommendations	
Alert variants	
Details	bootstrap.js v3.0.3-3.0.3

Web Server	
Alert group	**Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.
Recommendations	
Alert variants	
Details	bootstrap.js v3.0.3-3.0.3

Web Server	
Alert group	**Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.
Recommendations	
Alert variants	
Details	bootstrap.js v3.0.3-3.0.3

Web Server	
Alert group	**Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.
Recommendations	
Alert variants	

Details	bootstrap.js v3.0.3-3.0.3

Web Server	
Alert group	**Bootstrap Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.
Recommendations	
Alert variants	
Details	bootstrap.js v3.0.3-3.0.3

Web Server	
Alert group	**Development configuration files**
Severity	Medium
Description	One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.
Recommendations	Remove or restrict access to all configuration files acessible from internet.
Alert variants	

Details	Development configuration files:
	• http://10.67.253.121/template/plugins/jquery-validation/**package.json**
	`package.json => Grunt configuration file. Grunt is a JavaScript`
	• http://10.67.253.121/template/plugins/jquery-validation/**.travis.yml**
	`.travis.yml => Travis CI configuration file. Travis CI makes wor`

```
GET /template/plugins/jquery-validation/package.json HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Directory listings (verified)**
Severity	Medium
Description	Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.
Recommendations	You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.
Alert variants	

Details	Folders with directory listing enabled: • http://10.67.253.121/template/ • http://10.67.253.121/template/plugins/ • http://10.67.253.121/template/plugins/bootstrap/css/ • http://10.67.253.121/template/plugins/bootstrap/ • http://10.67.253.121/css/ • http://10.67.253.121/css/skins/ • http://10.67.253.121/css/skins/default/ • http://10.67.253.121/template/plugins/jquery-validation/ • http://10.67.253.121/template/plugins/jquery-validation/dist/ • http://10.67.253.121/backups/ • http://10.67.253.121/core/ • http://10.67.253.121/js/ • http://10.67.253.121/images/ • http://10.67.253.121/secret/ • http://10.67.253.121/uploads/ • http://10.67.253.121/css/skins/default/img/ • http://10.67.253.121/template/css/ • http://10.67.253.121/template/css/pages/ • http://10.67.253.121/images/fileicons/ • http://10.67.253.121/uploads/attachments/ • http://10.67.253.121/template/plugins/font-awesome/

```
GET /template/ HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

/index.php	
Alert group	**Host header attack**
Severity	Medium
Description	In many cases, developers are trusting the HTTP Host header value and using it to generate links, import scripts and even generate password resets links with its value. This is a very bad idea, because the HTTP Host header can be controlled by an attacker. This can be exploited using web-cache poisoning and by abusing alternative channels like password reset emails.
Recommendations	The web application should use the SERVER_NAME instead of the Host header. It should also create a dummy vhost that catches all requests with unrecognized Host headers. This can also be done under Nginx by specifying a non-wildcard SERVER_NAME, and under Apache by using a non-wildcard serverName and turning the UseCanonicalName directive on. Consult references for detailed information.
Alert variants	
Details	Host header **evilhostfy06NV5Q.com** was reflected inside an **FORM** tag (**action** attribute).

```
GET /index.php HTTP/1.1
Host: 10.67.253.121
X-Forwarded-Host: evilhostfy06NV5Q.com
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**Insecure HTTP Usage**
Severity	Medium
Description	It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.
Recommendations	It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information
Alert variants	
Details	

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**JQuery Prototype Pollution Vulnerability**
Severity	Medium
Description	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
Recommendations	
Alert variants	
Details	jquery v1.10.2-1.10.2

Web Server	
Alert group	**Password transmitted over HTTP**
Severity	Medium
Description	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
Recommendations	Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).
Alert variants	

Details	Forms with credentials sent in clear text: • http://10.67.253.121/ Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password] • http://10.67.253.121/index.php/login Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password] • http://10.67.253.121/index.php Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password] • http://10.67.253.121/index.php/js/app.js Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password] • http://10.67.253.121/index.php/index.php/login/restorePassword Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password] • http://10.67.253.121/index.php/ Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password] • http://10.67.253.121/index.php/index.php/login/ Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password] • http://10.67.253.121/index.php/js/ Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password] • http://10.67.253.121/index.php/index.php/ Form name: loginForm Form action: http://10.67.253.121/index.php/login Form method: POST Password input: login[password]

- http://10.67.253.121/index.php/login/

```
Form name: loginForm
Form action: http://10.67.253.121/index.php/login
Form method: POST
Password input: login[password]
```

```
GET / HTTP/1.1
Referer: http://10.67.253.121/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**SSL/TLS Not Implemented (verified)**
Severity	Medium
Description	This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
Recommendations	The site should send and receive data over a secure (HTTPS) connection.
Alert variants	
Details	

```
GET / HTTP/1.1
Referer: http://10.67.253.121/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Vulnerable JavaScript libraries**
Severity	Medium
Description	You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the 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	• **jQuery 1.10.2** ◦ URL: http://10.67.253.121/ ◦ Detection method: The library's name and version were determined based on its dynamic behavior. ◦ CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023 ◦ Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. ◦ References: ▪ https://github.com/jquery/jquery/issues/2432 ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ ▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ ▪ https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html ▪ https://jquery.com/upgrade-guide/3.5/ ▪ https://api.jquery.com/jQuery.htmlPrefilter/ ▪ https://www.cvedetails.com/cve/CVE-2020-11022/ ▪ https://github.com/advisories/GHSA-gxr4-xjj5-5px2 ▪ https://www.cvedetails.com/cve/CVE-2020-11023/ ▪ https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

```
GET / HTTP/1.1
Referer: http://10.67.253.121/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Vulnerable JavaScript libraries**
Severity	Medium
Description	You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the 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	• **jQuery Migrate 1.2.1** ◦ URL: http://10.67.253.121/template/plugins/jquery-migrate-1.2.1.min.js ◦ Detection method: The library's name and version were determined based on the file's name, and syntax fingerprint. ◦ CVE-ID: N/A ◦ Description: HTML injection ◦ References: ▪ http://bugs.jquery.com/ticket/11290 ▪ http://research.insecurelabs.org/jquery/test/

```
GET /template/plugins/jquery-migrate-1.2.1.min.js HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.
Recommendations	
Alert variants	
Details	jquery v1.10.2-1.10.2

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
Recommendations	
Alert variants	
Details	jquery v1.10.2-1.10.2

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
Recommendations	
Alert variants	
Details	jquery v1.10.2-1.10.2

Web Server	
Alert group	**Cookies Not Marked as HttpOnly (verified)**
Severity	Low

Description	One or more cookies don't 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 these cookies.
Alert variants	
Details	Cookies without HttpOnly flag set: • http://10.67.253.121/ `Set-Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng; path=/`

```
GET / HTTP/1.1
Referer: http://10.67.253.121/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Cookies with missing, inconsistent or contradictory properties (verified)**
Severity	Low
Description	At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.
Recommendations	Ensure that the cookies configuration complies with the applicable standards.
Alert variants	

Details	List of cookies with missing, inconsistent or contradictory properties:
	• http://10.67.253.121/
	Cookie was set with:
	`Set-Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng; path=/`
	This cookie has the following issues:
	` - Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`

```
GET / HTTP/1.1
Referer: http://10.67.253.121/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Documentation files**
Severity	Low
Description	One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.
Recommendations	Remove or restrict access to all documentation file acessible from internet.
Alert variants	

Details	Documentation files:
	• http://10.67.253.121/**readme.txt**
	File contents (first 100 characters):
	`qdPM`
	`open source project management software written in symfony frame`
	`http://qdpm.net`
	`INSTA ...`
	• http://10.67.253.121/template/plugins/jquery-validation/**README.md**
	File contents (first 100 characters):
	`[jQuery Validation Plugin](http://bassistance.de/jquery-plugins/`
	• http://10.67.253.121/template/plugins/jquery-validation/**changelog.txt**
	File contents (first 100 characters):
	`1.11.1 / 2013-03-22`
	`==========`
	`* Revert to also converting parameters of range method to ...`
	• http://10.67.253.121/core/**README**
	File contents (first 100 characters):
	`symfony sandbox`
	`==========`
	`Thank you for downloading the symfony sandbox. This pre-configur`

```
GET /readme.txt HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Missing Content-Type Header (verified)**
Severity	Low
Description	These page(s) 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 these page(s).
Alert variants	
Details	Pages where the content-type header is not specified: • http://10.67.253.121/core/LICENSE • http://10.67.253.121/core/README • http://10.67.253.121/core/config/databases.yml • http://10.67.253.121/core/symfony • http://10.67.253.121/template/plugins/jquery-validation/.travis.yml

```
GET /core/LICENSE HTTP/1.1
Referer: http://10.67.253.121/core/
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	One or more possibly sensitive directories were found. These resources are 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 these directories or remove them from the website.
Alert variants	
Details	Possible sensitive directories: • http://10.67.253.121/**uploads** • http://10.67.253.121/**secret** • http://10.67.253.121/**install** • http://10.67.253.121/**backups**

```
GET /uploads/ HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	

Alert group	**Possible sensitive files**
Severity	Low
Description	A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.
Recommendations	Restrict access to this file or remove it from the website.
Alert variants	
Details	Possible sensitive files: • http://10.67.253.121/install/**install.sql**

```
GET /install/install.sql HTTP/1.1
Accept: nlhhtjao/kroi
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Programming Error Messages**
Severity	Low
Description	This alert requires manual confirmation Acunetix found one or more error/warning messages. Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. These messages 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(s).
Recommendations	Verify that these page(s) are 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	Application error messages: • http://10.67.253.121/index.php/js/app.js **Fatal error** • http://10.67.253.121/index.php/js/app.js **Fatal error: Uncaught sfStopException in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php:96 Stack trace: #0 /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php(55): sfBasicSecurityFilter->forwardToLoginAction() #1 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfBasicSecurityFilter->execute(Object(sfFilterChain)) #2 /var/www/html/core/lib/vendor/symfony/lib/filter/sfRenderingFilter.class.php(33): sfFilterChain->execute() #3 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfRenderingFilter->execute(Object(sfFilterChain)) #4 /var/www/html/core/lib/vendor/symfony/lib/controller/sfController.class.php(238): sfFilterChain->execute() #5 /var/www/html/core/lib/vendor/symfony/lib/exception/sfError404Exception.class.php(28): sfController->forward('pageNotFound', 'index') #6 /var/www/html/core/lib/vendor/symfony/lib/controller/sfFrontWebController.class.php(52): sfError404Exception->printStackTrace() #7 /var/ww in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php on line 96 ** • http://10.67.253.121/index.php/index.php/login/restorePassword **Fatal error** • http://10.67.253.121/index.php/index.php/login/restorePassword **Fatal error: Uncaught sfStopException in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php:96 Stack trace: #0 /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php(55): sfBasicSecurityFilter->forwardToLoginAction() #1 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfBasicSecurityFilter->execute(Object(sfFilterChain)) #2 /var/www/html/core/lib/vendor/symfony/lib/filter/sfRenderingFilter.class.php(33): sfFilterChain->execute() #3 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfRenderingFilter->execute(Object(sfFilterChain)) #4 /var/www/html/core/lib/vendor/symfony/lib/controller/sfController.class.php(238): sfFilterChain->execute() #5 /var/www/html/core/lib/vendor/symfony/lib/exception/sfError404Exception.class.php(28): sfController->forward('pageNotFound', 'index') #6 /var/www/html/core/lib/vendor/symfony/lib/controller/sfFrontWebController.class.php(52): sfError404Exception->printStackTrace() #7 /var/ww in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php on line 96 ** • http://10.67.253.121/index.php/index.php/login/ **Fatal error** • http://10.67.253.121/index.php/index.php/login/ **Fatal error: Uncaught sfStopException in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilt**

**er.class.php:96 Stack trace: #0 /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php(55): sfBasicSecurityFilter->forwardToLoginAction() #1 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfBasicSecurityFilter->execute(Object(sfFilterChain)) #2 /var/www/html/core/lib/vendor/symfony/lib/filter/sfRenderingFilter.class.php(33): sfFilterChain->execute() #3 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfRenderingFilter->execute(Object(sfFilterChain)) #4 /var/www/html/core/lib/vendor/symfony/lib/controller/sfController.class.php(238): sfFilterChain->execute() #5 /var/www/html/core/lib/vendor/symfony/lib/exception/sfError404Exception.class.php(28): sfController->forward('pageNotFound', 'index') #6 /var/www/html/core/lib/vendor/symfony/lib/controller/sfFrontWebController.class.php(52): sfError404Exception->printStackTrace() #7 /var/ww in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php on line 96
**

- http://10.67.253.121/index.php/js/
  Fatal error

- http://10.67.253.121/index.php/js/
  **Fatal error: Uncaught sfStopException in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php:96 Stack trace: #0 /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php(55): sfBasicSecurityFilter->forwardToLoginAction() #1 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfBasicSecurityFilter->execute(Object(sfFilterChain)) #2 /var/www/html/core/lib/vendor/symfony/lib/filter/sfRenderingFilter.class.php(33): sfFilterChain->execute() #3 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfRenderingFilter->execute(Object(sfFilterChain)) #4 /var/www/html/core/lib/vendor/symfony/lib/controller/sfController.class.php(238): sfFilterChain->execute() #5 /var/www/html/core/lib/vendor/symfony/lib/exception/sfError404Exception.class.php(28): sfController->forward('pageNotFound', 'index') #6 /var/www/html/core/lib/vendor/symfony/lib/controller/sfFrontWebController.class.php(52): sfError404Exception->printStackTrace() #7 /var/ww in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php on line 96
**

- http://10.67.253.121/index.php/index.php/
  Fatal error

- http://10.67.253.121/index.php/index.php/
  Fatal error: Uncaught sfStopException in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php:96 Stack trace: #0 /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php(55): sfBasicSecurityFilter->forwardToLoginAction() #1 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfBasicSecurityFilter->execute(Object(sfFilterChain)) #2 /var/www/html/core/lib/vendor/symfony/lib/filter/sfRenderingFilter.cl

**ass.php(33): sfFilterChain->execute() #3 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfRenderingFilter->execute(Object(sfFilterChain)) #4 /var/www/html/core/lib/vendor/symfony/lib/controller/sfController.class.php(238): sfFilterChain->execute() #5 /var/www/html/core/lib/vendor/symfony/lib/exception/sfError404Exception.class.php(28): sfController->forward('pageNotFound', 'index') #6 /var/www/html/core/lib/vendor/symfony/lib/controller/sfFrontWebController.class.php(52): sfError404Exception->printStackTrace() #7 /var/ww in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php on line 96
**

- http://10.67.253.121/index.php/login/
  Fatal error

- http://10.67.253.121/index.php/login/
  **Fatal error: Uncaught sfStopException in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php:96 Stack trace: #0 /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php(55): sfBasicSecurityFilter->forwardToLoginAction() #1 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfBasicSecurityFilter->execute(Object(sfFilterChain)) #2 /var/www/html/core/lib/vendor/symfony/lib/filter/sfRenderingFilter.class.php(33): sfFilterChain->execute() #3 /var/www/html/core/lib/vendor/symfony/lib/filter/sfFilterChain.class.php(53): sfRenderingFilter->execute(Object(sfFilterChain)) #4 /var/www/html/core/lib/vendor/symfony/lib/controller/sfController.class.php(238): sfFilterChain->execute() #5 /var/www/html/core/lib/vendor/symfony/lib/exception/sfError404Exception.class.php(28): sfController->forward('pageNotFound', 'index') #6 /var/www/html/core/lib/vendor/symfony/lib/controller/sfFrontWebController.class.php(52): sfError404Exception->printStackTrace() #7 /var/ww in /var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php on line 96
**

```
GET /index.php/js/app.js?111 HTTP/1.1
Referer: http://10.67.253.121/index.php/login
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Content Security Policy (CSP) Not Implemented**
Severity	Informational

Description	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.
	
	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:
	
	`Content-Security-Policy:`
	`  default-src 'self';`
	`  script-src 'self' https://code.jquery.com;`
	
	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.

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	Paths without CSP header: • http://10.67.253.121/ • http://10.67.253.121/index.php • http://10.67.253.121/backups/ • http://10.67.253.121/core/ • http://10.67.253.121/images/ • http://10.67.253.121/install/ • http://10.67.253.121/secret/ • http://10.67.253.121/install/index.php • http://10.67.253.121/uploads/ • http://10.67.253.121/css/skins/default/img/ • http://10.67.253.121/js/ • http://10.67.253.121/images/fileicons/ • http://10.67.253.121/uploads/attachments/ • http://10.67.253.121/index.php/js/app.js • http://10.67.253.121/css/ • http://10.67.253.121/images/icons/ • http://10.67.253.121/js/cluetip1.2.5/ • http://10.67.253.121/uploads/users/ • http://10.67.253.121/images/icons/arrows/ • http://10.67.253.121/core/apps/ • http://10.67.253.121/js/jsgantt/

```
GET / HTTP/1.1
Referer: http://10.67.253.121/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Error page web server version disclosure**
Severity	Informational

Description	Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker. Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.
Alert variants	
Details	

```
GET /ySe4nI3x3T HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries**
Severity	Informational
Description	You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.
Recommendations	Upgrade to the latest version.
Alert variants	
Details	• **bootstrap.js 3.0.3** ◦ URL: http://10.67.253.121/template/plugins/bootstrap/js/bootstrap.min.js ◦ Detection method: The library's name and version were determined based on the file's contents. ◦ References: ▪ https://github.com/twbs/bootstrap/releases

```
GET /template/plugins/bootstrap/js/bootstrap.min.js HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries**
Severity	Informational
Description	You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.
Recommendations	Upgrade to the latest version.
Alert variants	

Details	• **Respond.js 1.1.0** ◦ URL: http://10.67.253.121/template/plugins/respond.min.js ◦ Detection method: The library's name and version were determined based on the file's contents. ◦ References: ▪ https://github.com/scottjehl/Respond/tags

```
GET /template/plugins/respond.min.js HTTP/1.1
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**Permissions-Policy header not implemented**
Severity	Informational
Description	The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.
Recommendations	
Alert variants	
Details	Locations without Permissions-Policy header: • http://10.67.253.121/ • http://10.67.253.121/index.php/login • http://10.67.253.121/index.php • http://10.67.253.121/backups/ • http://10.67.253.121/core/ • http://10.67.253.121/images/ • http://10.67.253.121/install/ • http://10.67.253.121/secret/ • http://10.67.253.121/install/index.php • http://10.67.253.121/uploads/ • http://10.67.253.121/icons/ • http://10.67.253.121/css/skins/default/img/ • http://10.67.253.121/js/ • http://10.67.253.121/images/fileicons/ • http://10.67.253.121/uploads/attachments/ • http://10.67.253.121/index.php/js/app.js • http://10.67.253.121/css/ • http://10.67.253.121/images/icons/ • http://10.67.253.121/js/cluetip1.2.5/ • http://10.67.253.121/uploads/users/ • http://10.67.253.121/images/icons/arrows/

```
GET / HTTP/1.1
Referer: http://10.67.253.121/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Web Server	
Alert group	**[Possible] Internal Path Disclosure (*nix)**
Severity	Informational
Description	One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks. This alert may be a false positive, manual confirmation is required.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	
Details	Pages with paths being disclosed: • http://10.67.253.121/index.php/js/app.js **/var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php** • http://10.67.253.121/index.php/index.php/login/restorePassword **/var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php** • http://10.67.253.121/index.php/index.php/login/ **/var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php** • http://10.67.253.121/index.php/js/ **/var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php** • http://10.67.253.121/index.php/index.php/ **/var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php** • http://10.67.253.121/index.php/login/ **/var/www/html/core/lib/vendor/symfony/lib/filter/sfBasicSecurityFilter.class.php**

```
GET /index.php/js/app.js?111 HTTP/1.1
Referer: http://10.67.253.121/index.php/login
Cookie: qdPM8=7u2cp5qdqpcbgdeiojlfu6jbng
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 10.67.253.121
Connection: Keep-alive
```

Scanned items (coverage report)

http://10.67.253.121/
http://10.67.253.121/core/config/
http://10.67.253.121/index.php

Vulnerabilities

Scan details

Scan information	
Start url	http://testasp.vulnweb.com/
Host	http://testasp.vulnweb.com/

Threat level

Acunetix Threat Level 4

One or more critical-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	21
Critical	4
High	6
Medium	4
Low	4
Informational	3

Affected items

/Login.asp	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **tfUName** was set to **-1' OR 3*2*1=6 AND 000880=000880 --** Tests performed: • -1' OR 2+880-880-1=0+0+0+1 -- => **TRUE** • -1' OR 3+880-880-1=0+0+0+1 -- => **FALSE** • -1' OR 3*2<(0+5+880-880) -- => **FALSE** • -1' OR 3*2>(0+5+880-880) -- => **FALSE** • -1' OR 2+1-1+1=1 AND 000880=000880 -- => **FALSE** • -1' OR 3*2=5 AND 000880=000880 -- => **FALSE** • -1' OR 3*2=6 AND 000880=000880 -- => **TRUE** • -1' OR 3*2*0=6 AND 000880=000880 -- => **FALSE** • -1' OR 3*2*1=6 AND 000880=000880 -- => **TRUE** Original value: **sOdPqaAH** **Proof of Exploit** SQL query - SELECT db_name() acuforum

```
POST /Login.asp?RetURL=/Default.asp%3F HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Content-Type: application/x-www-form-urlencoded
Content-Length: 81
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive

tfUName=-1'%20OR%203*2*1=6%20AND%20000880=000880%20--%20&tfUPass=u]H[ww6KrA9F.x-F
```

/Login.asp	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	
Details	URL encoded POST input **tfUPass** was set to **-1' OR 3*2*1=6 AND 000649=000649 --** Tests performed: • -1' OR 2+649-649-1=0+0+0+1 -- => **TRUE** • -1' OR 3+649-649-1=0+0+0+1 -- => **FALSE** • -1' OR 3*2<(0+5+649-649) -- => **FALSE** • -1' OR 3*2>(0+5+649-649) -- => **FALSE** • -1' OR 2+1-1+1=1 AND 000649=000649 -- => **FALSE** • -1' OR 3*2=5 AND 000649=000649 -- => **FALSE** • -1' OR 3*2=6 AND 000649=000649 -- => **TRUE** • -1' OR 3*2*0=6 AND 000649=000649 -- => **FALSE** • -1' OR 3*2*1=6 AND 000649=000649 -- => **TRUE** Original value: **u]H[ww6KrA9F.x-F** **Proof of Exploit** SQL query - SELECT db_name() acuforum

```
POST /Login.asp?RetURL=/Default.asp%3F HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Content-Type: application/x-www-form-urlencoded
Content-Length: 73
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive

tfUName=sOdPqaAH&tfUPass=-1'%20OR%203*2*1=6%20AND%20000649=000649%20--%20
```

/showforum.asp	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	

Details	URL encoded GET input **id** was set to **-1 OR 3*2*1=6 AND 000983=000983 --** Tests performed: • -1 OR 2+983-983-1=0+0+0+1 -- => **TRUE** • -1 OR 3+983-983-1=0+0+0+1 -- => **FALSE** • -1 OR 3*2<(0+5+983-983) -- => **FALSE** • -1 OR 3*2>(0+5+983-983) -- => **FALSE** • -1 OR 2+1-1+1=1 AND 000983=000983 -- => **FALSE** • -1 OR 3*2=5 AND 000983=000983 -- => **FALSE** • -1 OR 3*2=6 AND 000983=000983 -- => **TRUE** • -1 OR 3*2*0=6 AND 000983=000983 -- => **FALSE** • -1 OR 3*2*1=6 AND 000983=000983 -- => **TRUE** Original value: **0** **Proof of Exploit** SQL query - SELECT db_name() acuforum

```
GET /showforum.asp?id=-1%20OR%203*2*1=6%20AND%20000983=000983%20--%20 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

/showthread.asp	
Alert group	**SQL Injection (verified)**
Severity	Critical
Description	SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.
Recommendations	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.
Alert variants	

Details	URL encoded GET input **id** was set to **0-1; waitfor delay '0:0:6' --** Tests performed: • 0-1; waitfor delay '0:0:15' -- => **15.264** • 0-1; waitfor delay '0:0:6' -- => **6.284** • 0-1; waitfor delay '0:0:0' -- => **0.261** • 0-1; waitfor delay '0:0:15' -- => **15.266** • 0-1; waitfor delay '0:0:3' -- => **3.265** • 0-1; waitfor delay '0:0:0' -- => **0.263** • 0-1; waitfor delay '0:0:6' -- => **6.281** Original value: **0**

```
GET /showthread.asp?id=0-1;%20waitfor%20delay%20'0:0:6'%20--%20 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

/Search.asp	
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	URL encoded GET input **tfSearch** was set to **the"><script>6J8F(9620)</script>** The input is reflected inside a tag parameter between double quotes.

```
GET /Search.asp?tfSearch=the"><script>6J8F(9620)</script> HTTP/1.1
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

/showforum.asp	
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	URL encoded POST input **tfSubject** was set to **1--><ScRiPt >jjgM(9835)</ScRiPt><!--** The input is reflected inside a comment element.

```
POST /showforum.asp?id=0 HTTP/1.1
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive

tfSubject=1--><ScRiPt%20>jjgM(9835)</ScRiPt><!--&tfText=555
```

/showforum.asp	
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	URL encoded POST input **tfText** was set to **555'"()&%<zzz><ScRiPt >jjgM(9835)</ScRiPt>**

```
POST /showforum.asp?id=0 HTTP/1.1
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive

tfSubject=1&tfText=555'"()%26%25<zzz><ScRiPt%20>jjgM(9835)</ScRiPt>
```

/Templatize.asp	
Alert group	**Directory traversal (verified)**
Severity	High

Description	This script is vulnerable to directory traversal attacks. Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	

Details	URL encoded GET input **item** was set to **../../../../../../../../../../../../windows/win.ini**
	
	File contents found:
	
	`; for 16-bit app support`
	
	Proof of Exploit
	File - \windows\win.ini
	
	`; for 16-bit app support`
	`[fonts]`
	`[extensions]`
	`[mci extensions]`
	`[files]`
	`[Mail]`
	`MAPI=1`

```
GET /Templatize.asp?item=../../../../../../../../../../../../../../windows/win.ini
HTTP/1.1
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

/Templatize.asp	
Alert group	**Local File Inclusion**
Severity	High
Description	This script is vulnerable to file inclusion attacks. The script was found to reference and potentially retrieve files from user-specified locations. User input is not sufficiently validated or sanitized prior to being passed to the vulnerable script's include function.
Recommendations	Edit the source code to ensure that input is properly validated. Where is possible, it is recommended to make a list of accepted filenames and restrict the input to that list. For PHP, the option **allow_url_fopen** would normally allow a programmer to open, include or otherwise use a remote file using a URL rather than a local file path. It is recommended to disable this option from php.ini.
Alert variants	

Details	URL encoded GET input **item** was set to **Templatize.asp** Pattern found: <%@LANGUAGE="VBSCRIPT" CODEPAGE="1252"%> <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http <html><!-- InstanceBegin template="/Templates/MainTemplate.dwt.asp" <head> <!-- InstanceBeginEditable name="doctitle" --> <title>Untitled Document</title> <!-- InstanceEndEditable --> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859 <!-- InstanceBeginEditable name="head" --><!-- InstanceEndEditable .

```
GET /Templatize.asp?item=Templatize.asp HTTP/1.1
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

/Login.asp	
Alert group	**Weak password**
Severity	High
Description	This page is using a weak password. Acunetix was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.
Recommendations	Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.
Alert variants	
Details	Username: **test**, Password: **test**.

```
POST /Login.asp HTTP/1.1
Referer: http://testasp.vulnweb.com/Login.asp
Cookie: ASPSESSIONIDCSRSTCCA=EJEEAKLCPBNPOFEBLAOIIPBB;
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive

tfUName=test&tfUPass=test&=Login&
```

Web Server	
Alert group	**Insecure HTTP Usage**
Severity	Medium
Description	It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

Recommendations	It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information
Alert variants	
Details	

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

/Logout.asp	
Alert group	**Open Redirection**
Severity	Medium
Description	This endpoint is possibly vulnerable to URL redirection attacks. URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.
Recommendations	Your script should properly sanitize user input.
Alert variants	
Details	URL encoded GET input **RetURL** was set to **http://bxss.me**

```
GET /Logout.asp?RetURL=http://bxss.me HTTP/1.1
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**Password transmitted over HTTP**
Severity	Medium
Description	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
Recommendations	Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).
Alert variants	

Details	Forms with credentials sent in clear text:
	• http://testasp.vulnweb.com/Login.asp
	`Form name: <empty>`
	`Form action: <empty>`
	`Form method: POST`
	`Password input: tfUPass`
	• http://testasp.vulnweb.com/Register.asp
	`Form name: frmRegister`
	`Form action: <empty>`
	`Form method: POST`
	`Password input: tfUPass`

```
GET /Login.asp?RetURL=/Default.asp%3F HTTP/1.1
Referer: http://testasp.vulnweb.com/
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**SSL/TLS Not Implemented (verified)**
Severity	Medium
Description	This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
Recommendations	The site should send and receive data over a secure (HTTPS) connection.
Alert variants	
Details	

```
GET / HTTP/1.1
Referer: http://testasp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**Cookies Not Marked as HttpOnly (verified)**
Severity	Low
Description	One or more cookies don't 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 these cookies.
Alert variants	

Details	Cookies without HttpOnly flag set: • http://testasp.vulnweb.com/ `Set-Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE; path=`

```
GET / HTTP/1.1
Referer: http://testasp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**Cookies with missing, inconsistent or contradictory properties (verified)**
Severity	Low
Description	At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.
Recommendations	Ensure that the cookies configuration complies with the applicable standards.
Alert variants	

Details	List of cookies with missing, inconsistent or contradictory properties:
	• http://testasp.vulnweb.com/
	Cookie was set with:
	`Set-Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE; path=`
	This cookie has the following issues:
	`- Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`

```
GET / HTTP/1.1
Referer: http://testasp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**Microsoft IIS tilde directory enumeration**
Severity	Low

Description	It is possible to detect short names of files and directories which have an 8.3 file naming scheme equivalent in Windows by using some vectors in several versions of Microsoft IIS. For instance, it is possible to detect all short-names of ".aspx" files as they have 4 letters in their extensions. This can be a major issue especially for the .Net websites which are vulnerable to direct URL access as an attacker can find important files and folders that they are not normally visible.
Recommendations	Consult the "Prevention Technique(s)" section from Soroush Dalili's paper on this subject. A link to this paper is listed in the Web references section below.
Alert variants	
Details	

```
GET /jscripts/tiny_mce//*~1*/a.aspx?aspxerrorpath=/ HTTP/1.1
Cookie: ASPSESSIONIDCSRSTCCA=GPDEAKLCAKKPOPLCJNGJABPE
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**Version Disclosure (ASP.NET)**
Severity	Low
Description	The HTTP responses returned by this web application include anheader named **X-AspNet-Version**. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled.

Recommendations	Apply the following changes to the web.config file to prevent ASP.NET version disclosure:
	
	`<System.Web>`
	`  <httpRuntime enableVersionHeader="false" />`
	`</System.Web>`

Alert variants	
Details	Version information found: `2.0.50727`

```
GET /|~.aspx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**Content Security Policy (CSP) Not Implemented**
Severity	Informational

Description	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.
	
	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:
	
	`Content-Security-Policy:`
	`  default-src 'self';`
	`  script-src 'self' https://code.jquery.com;`
	
	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.

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	Paths without CSP header: • http://testasp.vulnweb.com/ • http://testasp.vulnweb.com/Login.asp • http://testasp.vulnweb.com/Templates/MainTemplate.dwt.asp • http://testasp.vulnweb.com/Templates/Login.asp • http://testasp.vulnweb.com/Templatize.asp • http://testasp.vulnweb.com/showforum.asp • http://testasp.vulnweb.com/Templates/Register.asp • http://testasp.vulnweb.com/Default.asp • http://testasp.vulnweb.com/Register.asp • http://testasp.vulnweb.com/Search.asp • http://testasp.vulnweb.com/showthread.asp

```
GET / HTTP/1.1
Referer: http://testasp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**Permissions-Policy header not implemented**
Severity	Informational
Description	The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.
Recommendations	
Alert variants	
Details	Locations without Permissions-Policy header: • http://testasp.vulnweb.com/ • http://testasp.vulnweb.com/Login.asp • http://testasp.vulnweb.com/Templates/MainTemplate.dwt.asp • http://testasp.vulnweb.com/Images/ • http://testasp.vulnweb.com/Templates/Login.asp • http://testasp.vulnweb.com/Templatize.asp • http://testasp.vulnweb.com/jscripts/tiny_mce/ • http://testasp.vulnweb.com/showforum.asp • http://testasp.vulnweb.com/cgi-bin/ • http://testasp.vulnweb.com/html/ • http://testasp.vulnweb.com/t/ • http://testasp.vulnweb.com/Templates/ • http://testasp.vulnweb.com/Templates/Register.asp • http://testasp.vulnweb.com/jscripts/tiny_mce/themes/simple/css/ • http://testasp.vulnweb.com/jscripts/ • http://testasp.vulnweb.com/Default.asp • http://testasp.vulnweb.com/jscripts/tiny_mce/langs/ • http://testasp.vulnweb.com/Register.asp • http://testasp.vulnweb.com/jscripts/tiny_mce/themes/simple/ • http://testasp.vulnweb.com/Search.asp • http://testasp.vulnweb.com/jscripts/tiny_mce/themes/

```
GET / HTTP/1.1
Referer: http://testasp.vulnweb.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Web Server	
Alert group	**Version Disclosure (IIS)**
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	Version information found: `Microsoft-IIS/8.5`

```
GET /|~.aspx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: testasp.vulnweb.com
Connection: Keep-alive
```

Scanned items (coverage report)

http://testasp.vulnweb.com/
http://testasp.vulnweb.com/Login.asp
http://testasp.vulnweb.com/Logout.asp
http://testasp.vulnweb.com/Search.asp
http://testasp.vulnweb.com/Templatize.asp
http://testasp.vulnweb.com/showforum.asp
http://testasp.vulnweb.com/showthread.asp

Vulnerabilities

Scan details

Scan information	
Start url	http://192.168.0.108
Host	http://192.168.0.108/

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	11
Critical	0
High	0
Medium	8
Low	0
Informational	3

Affected items

Web Server	
Alert group	**Directory listings (verified)**
Severity	Medium
Description	Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.
Recommendations	You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.
Alert variants	
Details	Folders with directory listing enabled: • http://192.168.0.108/assets/ • http://192.168.0.108/assets/css/ • http://192.168.0.108/assets/js/ • http://192.168.0.108/images/ • http://192.168.0.108/assets/fonts/

```
GET /assets/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.108
Connection: Keep-alive
```

Web Server	
Alert group	**Insecure HTTP Usage**
Severity	Medium
Description	It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.
Recommendations	It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information
Alert variants	
Details	

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.108
Connection: Keep-alive
```

Web Server	
Alert group	**JQuery Prototype Pollution Vulnerability**
Severity	Medium
Description	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
Recommendations	

Alert variants	
Details	jquery v1.11.3-1.11.3

Web Server	
Alert group	**SSL/TLS Not Implemented (verified)**
Severity	Medium
Description	This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
Recommendations	The site should send and receive data over a secure (HTTPS) connection.
Alert variants	
Details	

```
GET / HTTP/1.1
Referer: http://192.168.0.108/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.108
Connection: Keep-alive
```

Web Server	
Alert group	**Vulnerable JavaScript libraries**
Severity	Medium
Description	You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the 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	• **jQuery 1.11.3** ◦ URL: http://192.168.0.108/ ◦ Detection method: The library's name and version were determined based on its dynamic behavior. ◦ CVE-ID: CVE-2015-9251, CVE-2020-11022, CVE-2020-11023 ◦ Description: Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. ◦ References: ▪ https://github.com/jquery/jquery/issues/2432 ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ ▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ ▪ https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html ▪ https://jquery.com/upgrade-guide/3.5/ ▪ https://api.jquery.com/jQuery.htmlPrefilter/ ▪ https://www.cvedetails.com/cve/CVE-2020-11022/ ▪ https://github.com/advisories/GHSA-gxr4-xjj5-5px2 ▪ https://www.cvedetails.com/cve/CVE-2020-11023/ ▪ https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

```
GET / HTTP/1.1
Referer: http://192.168.0.108/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.108
Connection: Keep-alive
```

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.
Recommendations	
Alert variants	
Details	jquery v1.11.3-1.11.3

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Recommendations	
Alert variants	
Details	jquery v1.11.3-1.11.3

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
Recommendations	
Alert variants	
Details	jquery v1.11.3-1.11.3

Web Server	
Alert group	**Content Security Policy (CSP) Not Implemented**
Severity	Informational

Description	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.
	
	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:
	
	`Content-Security-Policy:`
	`  default-src 'self';`
	`  script-src 'self' https://code.jquery.com;`
	
	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.

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	Paths without CSP header: • http://192.168.0.108/ • http://192.168.0.108/elements.html • http://192.168.0.108/images/ • http://192.168.0.108/assets/fonts/ • http://192.168.0.108/assets/ • http://192.168.0.108/generic.html • http://192.168.0.108/index.html • http://192.168.0.108/assets/css/ • http://192.168.0.108/assets/js/

```
GET / HTTP/1.1
Referer: http://192.168.0.108/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.108
Connection: Keep-alive
```

Web Server	
Alert group	**Error page web server version disclosure**
Severity	Informational
Description	Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker. Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.
Recommendations	Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.
Alert variants	
Details	

```
GET /qahn0RAnTm HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.108
Connection: Keep-alive
```

Web Server	
Alert group	**Permissions-Policy header not implemented**
Severity	Informational

Description	The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.
Recommendations	
Alert variants	
Details	Locations without Permissions-Policy header: • http://192.168.0.108/ • http://192.168.0.108/elements.html • http://192.168.0.108/images/ • http://192.168.0.108/icons/ • http://192.168.0.108/assets/fonts/ • http://192.168.0.108/assets/ • http://192.168.0.108/generic.html • http://192.168.0.108/index.html • http://192.168.0.108/assets/css/ • http://192.168.0.108/assets/js/

```
GET / HTTP/1.1
Referer: http://192.168.0.108/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.108
Connection: Keep-alive
```

Scanned items (coverage report)

http://192.168.0.108/