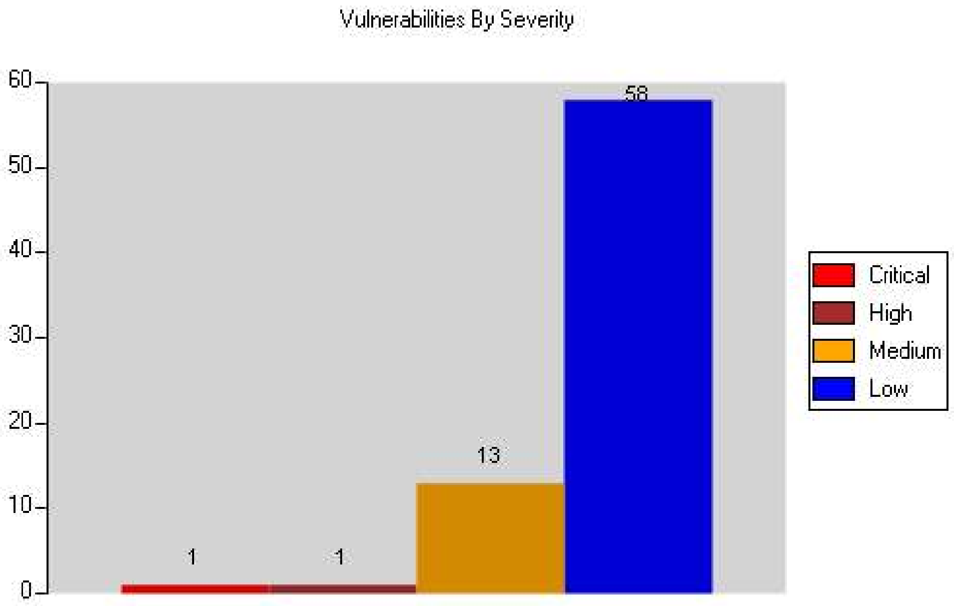
Hewlett Packard
Enterprise

HPE Fortify WebInspect

Multiple Reports

Web Application Assessment Report

Server: https://uat2-eservice.transglobe.com.tw:443



Critical

Insecure Transport: Weak SSL Cipher

Summary:

WebInspect has detected support for weak TLS/SSL ciphers on server **https://uat2-eservice.transglobe.com.tw:443/** .

The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols provide a mechanism to help protect authenticity, confidentiality and integrity of the data transmitted between a client and web server. The strength of this protection mechanism is determined by the authentication, encryption and hashing algorithms, collectively known as a cipher suite, chosen for the transmission of sensitive information over the TLS/SSL channel. Most Web servers support a range of such cipher suites of varying strengths. Using a weak cipher or an encryption key of insufficient length, for example, could allow an attacker to defeat the protection mechanism and steal or modify sensitive information.

If misconfigured, a web server could be manipulated into choosing weak cipher suites. Recommendations include updating the web server configuration to always choose the strongest ciphers for encryption.

Execution:

Each weak cipher was enumerated by establishing an SSL connection with the target host and specifying the cipher to test in the Client Hello message of the SSL handshake.

Implication:

A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current methods and resources. An attacker may be able to execute a man-in-the-middle attack which would allow them to intercept, monitor and tamper with sensitive data.

Fix:

Disable support for weak ciphers on the server. Weak ciphers are generally defined as:

- Any cipher with key length less than 128 bits
- Export-class cipher suites
- NULL ciphers
- Ciphers that support unauthenticated modes
- Ciphers assessed at security strenghts below 112 bits
- All RC4 ciphers
- All 64-bit block ciphers

The following ciphers supported by the server are weak and should be disabled:

- **TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)**

The weak cipher list above also includes ciphers that enable conditions for SWEET32 cipher attacks. The vulnerability affects all 64-bit block ciphers such as 3DES and Blowfish. The vulnerability is independent of the number of keys and/or the key length used in the cipher. It could allow attackers to obtain cleartext data from long-lived encrypted sessions. The vulnerability is identified by CVE-2016-2183 and CVE-2016-6329.

The following 64-bit block ciphers should be removed from the target server configuration to prevent SWEET32 attacks:

- **TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)**

- For Apache, modify the following lines in httpd.conf or ssl.conf:

- SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!NULL:!RC4:!RC2:!DES:!3DES+HIGH:+MEDIUM

- For IIS, please refer to Microsoft Knowledge Base Articles:

- Article ID: 187498
- Article ID: 245030 and
- Security Guidance for IIS
- Article ID: 2868725

- For other servers, please refer to vendor specific documentation.

The following ciphers supported by the server should provide adequate protection and may be left enabled:

- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)**
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)**
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)**
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)**
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)**
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)**

Reference:

OWASP:
Transport Layer Protection Cheat Sheet

PCI Security Standards Council:
PCI DSS v3.1

CVE
CVE-2013-2566
CVE-2016-2183
CVE-2016-6329

NIST
NIST Special Publication 800-131A

Microsoft:
Knowledge Base Article ID: 2868725
Knowledge Base Article ID: 187498
Knowledge Base Article ID: 245030
Security Guidance for IIS

Apache:
SSL/TLS Strong Encryption: FAQ

RC4:
New RC4 Attack

ACM CCS '16
On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN

File Names:
- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

High **Password Management: Weak Password Policy**

Summary:

Authentication is an important aspect of security. Password authentication requires users to present login credentials as evidence to validate their identity before granting them access to server resources. The reliability of the authentication process depends on the security of the login credentials. Password policies that ensure users create strong passwords are therefore crucial to deploying secure websites. Password strength is a measure of the effectiveness it provides in resisting guessing and brute force attacks. Some of the parameters that help define the password strength include password characteristics such as password length, complexity and randomness.

WebInspect has detected that the current website does not meet the basic guidelines for a secure password.

*The password value used in Login Macro **LoginMacro1** fails to meet these requirements.*

The password does not meet the minimum length requirement of 8 characters.
The password does not contain both uppercase and lowercase alphabets.
The password is not alphanumeric.
The password does not contain special characters.
The password does not contain the required number of tokens. Set of [Letters], [Numbers], [Special characters] are defined as three distinct tokens in WI. To increase the password entropy, it is recommended that the password contain a minimum of 4 of these tokens in any combination.

Note: The assumption is that the username / password used during pen-testing meet the username/password requirement for the web application when deployed live.

Implication:

System security is compromised by using weak passwords that can be easily guessed or are an easy target to brute force attacks. Authentication systems fail on compromised passwords as they cannot distinguishbetween impostors and authentic users of the system. Thus, compromising the integrity and confidentiality of the system resources and data.

Fix:

The effective strength of the password can be increased by enforcing rules that make the password random and harder to guess.
At a minimum, the password policy should adhere to the following rules:

- The password is at least 8 characters long.
- The password is alphanumeric and contain both letters and numbers.
- The password is a mix of uppercase and lowercase letters.
- The password contains special characters such as #,$ etc
- The password should not contain contextual information such as login credentials, website name etc
- In addition the password strength can be increased by enforcing rules that increase the password randomness. For example, you could require a password have a minimum of 4 tokens, where a token is defined as a set of either [letters], [numbers] or special characters. It is recommended that you implement a password policy that helps increase the password entropy and hence the password strength.

Reference:

NIST Computer Security
Estimating Password Strength
NIST Guide to Enterprise Password Management
Special Publication 800-118
OWASP
Authentication Cheat Sheet
Bruce Schneier - Choosing Secure Passwords
Choosing Secure Passwords

File Names:
- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Medium **Poor Error Handling: Unhandled Exception**

Summary:

Unhandled exceptions are circumstances in which the application has received user input that it did not expect and doesn't know how to deal with. In many cases, an attacker can leverage the conditions that cause these errors in order to gain unauthorized access to the system. Recommendations include designing and adding consistent error-handling mechanisms that are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

Implication:

Exception error messages may contain the location of the file in which the offending function is located. This may disclose the webroot's absolute path as well as give the attacker the location of application include files or configuration information. It may even disclose the portion of code that failed. In most cases, it will be the result of the web application attempting to use an invalid client-supplied argument in a SQL statement, which means that SQL injection will be possible. If so, an attacker will at least be able to read the contents of the entire database arbitrarily. Depending on the database server and the SQL statement, deleting, updating and adding records and executing arbitrary commands may also be possible. If a software bug or bug is responsible for triggering the error, the potential impact will vary, depending on the circumstances. The location of the application that caused the error can be useful in facilitating other kinds of attacks. If the file is a hidden or include file, the attacker may be able to gain more information about the mechanics of the web application, possibly even the source code. Application source code is likely to contain usernames, passwords, database connection strings and aids the attacker greatly in discovering new vulnerabilities.

Fix:

For Security Operations:

Unknown application testing seeks to uncover new vulnerabilities in both custom and commercial software. Because of this, there are no specific patches or descriptions of this issue. Please note that this vulnerability may be a false positive if the page it is flagged on is technical documentation.However, follow these recommendations to help ensure a secure web application:

- **Use Uniform Error Codes:** Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by using error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Use consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- **Informational Error Messages:** Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft an attack.
- **Proper Error Handling:** Use generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be used by an attacker when orchestrating an attack.

For Development:

This problem arises from the improper validation of characters that are accepted by the application. Any time a parameter is passed into a dynamically-generated web page, you must assume that the data could be incorrectly formatted. The application should contain sufficient logic to handle any situation in which a parameter is not being passed or is being passed incorrectly. Keep in mind how the data is being submitted, as a result of a GET or a POST. Additionally, to develop secure and stable code, treat cookies the same as parameters. The following recommendations will help ensure that you are delivering secure web applications.

- **Stringently define the data type:** Stringently define the data type (a string, an alphanumeric character, etc.) that the application will accept. Validate input for improper characters. Adopt the philosophy of using what is good rather than what is bad. Define the allowed set of characters. For instance, if a field is to receive a number, allow that field to accept only numbers. Define the maximum and minimum data lengths that the application will accept.
- **Verify parameter is being passed:** If a parameter that is expected to be passed to a dynamic Web page is omitted, the application should provide an acceptable error message to the user. Also, never use a parameter until you have verified that it has been passed into the application.
- **Verify correct format:** Never assume that a parameter is of a valid format. This is especially true if the parameter is being passed to a SQL database. Any string that is passed directly to a database without first being checked for proper format can be a major security risk. Also, just because a parameter is normally provided by a combo box or hidden field, do not assume the format is correct. A hacker will first try to alter these parameters while attempting to break into your site.
- **Verify file names being passed in via a parameter:** If a parameter is being used to determine which file to process, never use the file name before it is verified as valid. Specifically, test for the existence of characters that indicate directory traversal, such as .../, c:\, and /.
- **Do not store critical data in hidden parameters:** Many programmers make the mistake of storing critical data in a hidden parameter or cookie. They assume that since the user doesn't see it, it's a good place to store data such as price, order number, etc. Both hidden parameters and cookies can be manipulated and returned to the server, so never assume the client returned what you sent via a hidden parameter or cookie.

For QA:

From a testing perspective, ensure that the error handling scheme is consistent and does not reveal private information about your web application. A seemingly innocuous piece of information can provide an attacker the means to discover additional information that can be used to conduct an attack. Make the following observations:

- Do you receive the same type of error for existing and non-existing files?
- Does the error include phrases (such as "Permission Denied") that could reveal the existence of a file?

Reference:

Web Application Security Whitepaper:
http://download.hpsmartupdate.com/asclabs/security_at_the_next_level.pdf

Processing Unhandled Exceptions:
http://www.asp.net/(S(sf10gzjodvrpce55el2p5cnk))/learn/hosting/tutorial-12-cs.aspx

Managing Unhandled Exceptions:
http://www.informit.com/articles/article.aspx?p=32081&seqNum=3

File Names:

- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/Home/HomePage.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Medium

Cookie Security: Cookie Not Sent Over SSL

Summary:

This policy states that any area of the website or web application that contains sensitive information or access to privileged functionality such as remote site administration requires that all cookies are sent via SSL during an SSL session. The URL: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml has failed this policy. If a cookie is marked with the "secure" attribute, it will only be transmitted if the communications channel with the host is a secure one. Currently this means that secure cookies will only be sent to HTTPS (HTTP over SSL) servers. If secure is not specified, a cookie is considered safe to be sent in the clear over unsecured channels.

Fix:

For Development:
This issue will ultimately need to be rectified by your Network or Security Operations team. If necessary, implement the change in your development environment.

For Security Operations:

IIS 4.0 and 5.0 Fix Information:
http://support.microsoft.com/default.aspx?scid=kb;en-us;274149

Remediation for IIS 6.x:
http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0d49cbc8-10e1-4fa8-ba61-c34e524a3ae6.mspx?mfr=true
http://msdn2.microsoft.com/en-us/library/ms998310.aspx

Require SSL for an Authentication Cookie (IIS 7):
http://technet.microsoft.com/en-us/library/cc771633(WS.10).aspx

AnonymousIdentificationSection Class [IIS 7]:
http://msdn.microsoft.com/en-us/library/ms689482.aspx

Use the following links to remediate this issue on an Apache server:
http://search.cpan.org/~jkrasnoo/ApacheCookieEncrypted-0.03/Encrypted.pm
http://hc.apache.org/httpclient-3.x/apidocs/org/apache/commons/httpclient/class-use/Cookie.html

For QA:
This issue will ultimately need to be rectified by your Network or Security Operations team. If necessary, implement the change in your testing environment.

Reference:

General Information:
[The Unofficial Cookie FAQ]

File Names:	● https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Medium **Cross-Frame Scripting**

Summary:

A Cross-Frame Scripting (XFS) vulnerability can allow an attacker to load the vulnerable application inside an HTML iframe tag on a malicious page. The attacker could use this weakness to devise a Clickjacking attack to conduct phishing, frame sniffing, social engineering or Cross-Site Request Forgery attacks.

Clickjacking
The goal of a Clickjacking attack is to deceive the victim user into interacting with UI elements of the attacker's choice on the target web site without her knowledge and in turn executing privileged functionality on the victim's behalf. To achieve this goal, the attacker must exploit the XFS vulnerability to load the attack target inside an iframe tag, hide it using Cascading Style Sheets (CSS) and overlay the phishing content on the malicious page. By placing the UI elements on the phishing page to overlap with those on the page targeted in the attack, the attacker can ensure that the victim is forced to interact with the UI elements on the target page not visible to the victim.
WebInspect has detected a response containing one or more forms that accept user input but is missing XFS protection.

An effective frame-busting technique was not observed while loading this page inside a frame.

Execution:

Create a test page containing an HTML <iframe> tag whose **src** attribute is set to https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml. Successful framing of the target page indicates the application's susceptibility to XFS.
Note that WebInspect will report only one instance of this check across each host within the scope of the scan. The other visible pages on the site may, however, be vulnerable to XFS as well and hence should be protected against it with an appropriate fix.

Implication:

A Cross-Frame Scripting weakness could allow an attacker to embed the vulnerable application inside an iframe. Exploitation of this weakness could result in:

Hijacking of user events such as keystrokes
Theft of sensitive information
Execution of privileged functionality through combination with Cross-Site Request Forgery attacks

Fix:

Browser vendors have introduced and adopted a policy-based mitigation technique using the X-Frame-Options header. Developers can use this header to instruct the browser about appropriate actions to perform if their site is included inside an iframe. Developers must set the X-Frame-Options header to one of the following permitted values:

- DENY
Deny all attempts to frame the page
- SAMEORIGIN
The page can be framed by another page only if it belongs to the same origin as the page being framed
- ALLOW-FROM origin
Developers can specify a list of trusted origins in the origin attribute. Only pages on origin are permitted to load this page inside an iframe

Developers must **also** use client-side frame busting JavaScript as a protection against XFS. This will enable users of older browsers that do not support the X-Frame-Options header to also be protected from clickjacking attacks.

Reference:

HP 2012 Cyber Security Report
[The X-Frame-Options header - a failure to launch]

Server Configuration:
[IIS]
[Apache, nginx]

Specification:
[X-Frame-Options IETF Draft]

OWASP:
[Clickjacking]

Frame Busting:
[Busting Frame Busting: A Study of Clickjacking Vulnerabilities on Popular Sites]
[OWASP: Busting Frame Busting]

File Names:	● https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml

Medium

Privacy Violation: Inconsistent Feedback

Summary:

When entering an invalid username or password during a login, an application may provide meaningful feedback through a response discrepancy. For the potential attacker, this discrepancy increases the chances of a successful brute force attack against the site's authentication.

Execution:

Try logging into the application twice, once with an incorrect username and another time with an incorrect password. A generic error message for both attempts indicates a secure application. On the other hand, if there is a difference in the error messages, the application may be providing information that could be used in a brute-force attack.

Implication:

Consider an application that takes an email address/username and a password. If the application provides different error messages for a non-existent email address and an incorrect password, it will enable an attacker to submit multiple email addresses and learn about the ones that are actually registered to the application. Being able to enumerate users in an application may enable an attacker to perform a more efficient brute force attack.

Fix:

Applications should not indicate specifically whether a user account or password was incorrect, rather a very generic login failure message should be used. For example, during a new user registration or forgotten password function, no meaningful message should be returned to the requestor, rather an email should be sent to the account in question with details of how to reset a forgotten password or reclaim an account.

Reference:

OWASP Guide to Authentication
https://www.owasp.org/index.php/Guide_to_Authentication

Username Enumeration Vulnerabilities
http://www.gnucitizen.org/blog/username-enumeration-vulnerabilities

File Names:

- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Medium

Insecure Transport: Weak SSL Protocol

Summary:

HPE Security Fortify WebInspect has detected support for Transport Layer Security Protocol (TLS) 1.1 protocol on the target server. NIST publication 800-52 revision 1 recommends all web applications to prefer Transport Layer Security Protocol version 1.2 (TLS 1.2) and mandates government agencies to develop a migration plan for TLS1.2 by January 2015. TLS1.1 mandates a combination of MD5 and SHA1 for the hash function, which leads to conclusion that strength of TLS1.1 depends largely on the strength of SHA1. MD5 is generally known to be weak. SHA1 use is being phased out. NIST Special Publication 800-131A deprecated the use of SHA-1 in digital signature starting January 2014.

Execution:

The list of supported SSL/TLS protocols can be obtained by running the server analyzer tool from HPE security toolkit supplied with HPE Security Fortify WebInspect against the target server.

Implication:

Weak TLS/SSL protocols may exhibit any or all of the following properties:

- No protection against man-in-the-middle (MitM) attacks
- Same key used for authentication and encryption
- Weak message authentication control
- No protection against TCP connection closing

These properties can allow an attacker to intercept, modify and tamper with sensitive data.

Fix:

Have a migration plan in place for all sites to exclusively use TLS1.2 and above. Disable support for the TLS 1.1 protocol on the server. Instead, TLSv1.2 and above should be used.

- For Apache, modify the following lines in the server configuration
- SSL Protocol ALL –SSLv2 -SSLv3 -TLSv1 –TLSv1.1

- For Nginx, modify the following lines in server configuration:

- SSL_Protocols TLSv1.2

- For IIS, please refer to Microsoft Knowledge Base Articles:

  - https://technet.microsoft.com/library/security/3009008

For other servers, please refer to vendor specific documentation.

Reference:

NIST Special Publication 800-131A
NIST Special Publication 800-52r1

File Names:

- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Low **Cookie Security: HTTPOnly not Set**

Summary:

The web application does not utilize HTTP only cookies. This is a new security feature introduced by Microsoft in IE 6 SP1 to mitigate the possibility of a successful Cross-Site scripting attack by not allowing cookies with the HTTP only attribute to be accessed via client-side scripts. Recommendations include adopting a development policy that includes the utilization of HTTP only cookies, and performing other actions such as ensuring proper filtration of user-supplied data, utilizing client-side validation of user supplied data, and encoding all user supplied data to prevent inserted scripts being sent to end users in a format that can be executed.

Reference:

References:
https://social.msdn.microsoft.com/Search/en-US?query=HTTPOnly%20Cookie&emptyWatermark=true&ac=5

File Names:

- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Low **Web Server Misconfiguration: Server Error Message**

Summary:

A server error response was detected. The server could be experiencing errors due to a misbehaving application, a misconfiguration, or a malicious value sent during the auditing process. While error responses in and of themselves are not dangerous, per se, the error responses give attackers insight into how the application handles error conditions. Errors that can be remotely triggered by an attacker can also potentially lead to a denial of service attack or other more severe vulnerability. Recommendations include designing and adding consistent error handling mechanisms which are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

Implication:

The server has issued a 500 error response. While the body content of the error page may not expose any information about the technical error, the fact that an error occurred is confirmed by the 500 status code. Knowing whether certain inputs trigger a server error can aid or inform an attacker of potential vulnerabilities.

Fix:

For Security Operations:

Server error messages, such as "File Protected Against Access", often reveal more information than intended. For instance, an attacker who receives this message can be relatively certain that file exists, which might give him the information he needs to pursue other leads, or to perform an actual exploit. The following recommendations will help to ensure that a potential attacker is not deriving valuable information from any server error message that is presented.

- Uniform Error Codes: Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by utilizing error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Have consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- Informational Error Messages: Ensure that error messages do not reveal too much information. Complete or partial

paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft a method of attack.

- Proper Error Handling: Utilize generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be utilized by an attacker when orchestrating an attack.

Removing Detailed Error Messages

Find instructions for turning off detailed error messaging in IIS at this link:

http://support.microsoft.com/kb/294807

For Development:

From a development perspective, the best method of preventing problems from arising from server error messages is to adopt secure programming techniques that prevent problems that might arise from an attacker discovering too much information about the architecture and design of your web application. The following recommendations can be used as a basis for that.

- Stringently define the data type (for instance, a string, an alphanumeric character, etc) that the application will accept.
- Use what is good instead of what is bad. Validate input for improper characters.
- Do not display error messages to the end user that provide information (such as table names) that could be utilized in orchestrating an attack.
- Define the allowed set of characters. For instance, if a field is to receive a number, only let that field accept numbers.
- Define the maximum and minimum data lengths for what the application will accept.
- Specify acceptable numeric ranges for input.

For QA:

The best course of action for QA associates to take is to ensure that the error handling scheme is consistent. Do you receive a different type of error for a file that does not exist as opposed to a file that does? Are phrases like "Permission Denied" utilized which could reveal the existence of a file to an attacker? Inconsistent methods of dealing with errors gives an attacker a very powerful way of gathering information about your web application.

Reference:

Apache:
Security Tips for Server Configuration
Protecting Confidential Documents at Your Site
Securing Apache - Access Control

Microsoft:
How to set required NTFS permissions and user rights for an IIS 5.0 Web server
Default permissions and user rights for IIS 6.0
Description of Microsoft Internet Information Services (IIS) 5.0 and 6.0 status codes

File Names:

- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml
- https://uat2-eservice.transglobe.com.tw:443/<script>alert('TRACK');</script>
- https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/Home/HomePage.xhtml

---

Low **Privacy Violation: Autocomplete**

Summary:

Most recent browsers have features that will save password field content entered by users and then automatically complete password entry the next time the field are encountered. This feature is enabled by default and could leak password since it is stored on the hard drive of the user. The risk of this issue is greatly increased if users are accessing the application from a shared environment. Recommendations include setting autocomplete to "off" on all your password fields.

Please Note: Recent versions of most browsers, as noted below, now ignore the autocomplete="off" attribute for password fields in html forms. Users are allowed to decide the password policy at their own discretion using the password manager. Although setting is ineffective on these versions of browsers, it would continue to protect website users of earlier versions of these and other browsers that support this attribute.

Browsers NOT Supporting autocomplete="off":

Internet Explorer version 11 or above
Firefox version 30 or above
Chrome version 34 or above
For other browsers, please refer to vendor specific documentation

Execution:

To verify if a password filed is vulnerable, first make sure to enable the autocomplete in your browser's settings, and then input the other fileds of the form to see whether the password is automatically filled. If yes, then it's vulnerable, otherwise, not. You may need to do it twice in case it is the first time you type in the credential in your browser.

Please Note: That some modern browsers no longer support this attribute as summarized above. Verification should be done using a browser that supports this attribute.

Implication:

When autocomplete is enabled, hackers can directly steal your password from local storage.

Fix:

From the web application perspective, the autocomplete can be turned at the form level or individual entry level by defining the attribute AUTOCOMPLETE="off".

Reference:

Microsoft:
Autocomplete Security

File Names:

- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Low **Cache Management: Insecure Policy**

Summary:

WebInspect has detected a potentially unsafe cache control policy for secure content. While content transmitted over an SSL/TLS channel is expected to guarantee confidentiality, administrators must nonetheless ensure that caching of sensitive content is disabled unless absolutely needed. The misconception that secure content caching is disabled by default by user-agents could cause the application to fail the organization’s cache policy by leaving the secure content cacheable by browsers. Unsafe specification such as Cache-Control: public would instruct the browser to persistently cache the content on the hard drive. Caching can be prevented by specifying one of the following three directives in the response headers

- Cache-control: private
- Cache-Control: no-cache
- Cache-Control: no-store

Execution:

Send a request to https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerBankAccountSetting.xhtml and inspect the Cache-Control header value.

Implication:

Insecure caching policies could lead to content spoofing or information theft.

SSL provides secure encrypted channel to transfer information from source to user. The information server over SSL is considered sensitive and trusted to be only available to requestor. However, caching these content on disk in temporary internet files or in intermediate proxy server can compromise that trust by exposing it to everyone who has access to these temporary storage or proxy cache. Content served over SSL should have cache disabled.

Fix:

Set Cache-Control directive to private, no-cache and/or no-store.

private
This directive allows the server to prevent a shared cache from caching responses that are intended for a single user. The mechanism can be used to ensure that privileged information is not accidentally leaked to unauthorized users. The directive may still allow caching of responses by non-shared caches.

no-cache
For sensitive resources requiring user authentication, servers can send the no-cache directive to prevent caches from serving a cached response without first requiring the user agent to validate the user identity. This directive can be specified with or without field names. When no field names are included, this directive applies to the entire request or response.
When one or more field names are specified in the no-cache directive, the response is can be cached but the specified field(s) must be excluded. If the response must include the specified field, then the cache must ensure that the request triggers a

revalidation with the origin server.
Example: Cache-Control: no-cache="Set-Cookie"
This directive can be used to ensure sensitive information leakage by requiring the server to confirm the user identity before serving the protected information.

no-store
To completely disable caching of requests or responses, the server must specify the no-store directive in the Cache-Control header. This directive applies to the entire request and response regardless of whether the directive is sent in the request or the response.

Reference:

Server Configuration:
IIS
Apache

HTTP 1.1 Specification:
HTTP Header Field Definitions

OWASP:
Browser Cache FAQ

HTTP Caching:
Tutorial

File Names:

- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerBankAccountSetting.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/jquery/jquery-plugins.js.xhtml?l
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/fonts/MaterialIcons-Regular.woff
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPolicyChangeNotice.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-l
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/primefaces-extensions.js.xhtml?l
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/blockui/blockui.css.xhtml?ln=pri
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/layout.js.xhtml?ln=barcelona-
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPolicyList.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerCreditCardMaintain.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/sas.js.xhtml?ln=barcelona-lay
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerIncomeTax.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/core.js.xhtml?ln=primefaces&v=6.
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/transglobe/img/logo.ico.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerClaimsRecordQuery.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/barcelona-layout/images/favicon.
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/fa/fontawesome-webfont.ttf.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerECServiceOpen.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/Home/HomePage.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/exception-style.css.xhtml?ln
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/nanoscroller.js.xhtml?ln=barc
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerLoanRecordQuery.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/nanoscroller.css.xhtml?ln=ba
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/animate.css.xhtml?ln=barcelo
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPayment.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerContractChangeQuery.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerOnlinePay01.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/layout-login.css.xhtml?ln=tr
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/idlemonitor/idlemonitor.js.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/components.js.xhtml?ln=primeface

- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/fa/fontawesome-webfont.woff.xhtm
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPolicyChangeAndElectronicNotice.x
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/JQueryDatePickerTW.js.xhtml?l
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/blockui/blockui.js.xhtml?ln=prim
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/ripple.css.xhtml?ln=barcelon
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/jquery/jquery.js.xhtml?ln=primef
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPolicyCertificationServer.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/jquery-ui.js.xhtml?ln=barcelo
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/header_footer_login.css.xhtm
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/ripple.js.xhtml?ln=barcelona-
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/localzhTW.js.xhtml?ln=barcelo
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/layout-blue.css.xhtml?ln=bar
- https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/Home/ChangPwd.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/theme.css.xhtml?ln=primefaces-ba
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/header_footer_MainSouth.css.
- https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/fa/font-awesome.css.xhtml?ln=pri
- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/components.css.xhtml?ln=primefac
- https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Low

Insecure Transport: HSTS Not Set

Summary:

Http Strict Transport Security (HSTS) policy enables web applications to enforce web browsers to restrict communication with the server over an encrypted SSL/TLS connection for a set period. Policy is declared via special Strict Transport Security response header. Encrypted connection protects sensitive user and session data from attackers eavesdropping on network connection.
Consider following attack scenarios:

- Users often omit the URI scheme i.e. https:// when typing a URL in location bar to access a website. Also third party websites can link to the site using the “http” scheme instead of "”https”. This could result in an initial connection to a HTTPS-enabled site over an unencrypted channel. An eavesdropping attacker can hijack this unencrypted connection and replace the intended use of HTTPS protocol with HTTP in an attack known as SSLStrip, granting unauthorized access to all subsequent traffic.
- Websites often transfer non-sensitive resources such as help documents over an unencrypted HTTP connection. Any cookies without a secure flag are sent along with such requests potentially disclosing sensitive user and session data to eavesdropper.
- Man-in-the-Middle attacks that exploit user tendencies to override invalid certification warnings, e.g. SSLSniff.

For web sites configured with an accurate HSTS policy, browsers automatically upgrade any HTTP connections to HTTPS. Furthermore, browsers prevent users from overriding any host certificate warnings. HSTS offers an effective defense against above attack scenarios.

Execution:

Access location https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-layout and notice the absence of the Strict Transport Security header in the HTTP response.

Implication:

A successful MiTM attack such as SSLStrip or SSLsniff can lead to the compromise of sensitive user data such as financial information, Social Security Number, personal information etc. as well as grant unauthorized access to user accounts enabling attackers to perform privileged actions on client’s behalf.

Fix:

Configure the web application under test to include Strict Transport Security header in every response generated by an HTTPS -enabled site. Any HTTP version of site on the same domain should permanently redirect to the secure encrypted site. Header should not be added to HTTP response as browsers will ignore it.

It is important to note that this header does not prevent from above mentioned attack scenarios during the very first connection to the site or any connections established after the set period has expired. To prevent such a scenario, the site must be added to the pre-loaded HSTS hosts list embedded in both Google Chrome and Mozilla Firefox browsers.

Reference:

http://tools.ietf.org/html/rfc6797

File Names:

- https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-l

Server: https://uat2-eservice.transglobe.com.tw:443

Critical Issues

Insecure Transport: Weak SSL Cipher (11285)

View Description

CWE: 319,326,327

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Request:

```
GET /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Crawl.EventMacro.Startup";
SID="BCEAF30F249217B459AC90AFE417D8DC"; SessionType="StartMacro";
CrawlType="None";
X-RequestManager-Memo: sid="29"; smi="0"; Category="EventMacro.Login";
MacroName="LoginMacro1";
X-Request-Memo: ID="4a97cb7d-22fd-444e-8c43-67f52f82eb8a"; tid="81";
Pragma: no-cache
Cookie: CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Length: 14766
Set-Cookie: JSESSIONID=qKVx1HRD3M6Z5WeFd314lMYQ; Path=/cs; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
Date: Sat, 30 Mar 2019 06:00:30 GMT
Set-Cookie: BIGipServerpool_UAT2-ESERVICE=1799570186.9760.0000; path=/

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml"><head id="j_idt2">
      <meta http-equiv="X-UA-Compatible" content="IE=9; IE=EDGE" />
      <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
            <meta http-equiv="Content-Type" content="text/html; charset=UTF-
8" />
            <meta http-equiv="refresh" content="300" />
            <meta name="viewport" content="width=device-width, initial-
scale=1.0, maximum-scale=1.0, user-scalable=yes" />
            <meta name="format-detection" content="telephone=no" />
            <meta name="apple-mobile-web-app-capable" content="yes" />
            <meta name="apple-mobile-web-app-status-bar-style"
content="black" />
            <meta name="keywords" content=", , ,
, , " /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/theme.css.xhtml?ln=primefaces-barcelona-
blue" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/fa/font-awesome.css.xhtml?
ln=primefaces&amp;v=6.1" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/layout-login.css.xhtml?
ln=transglobe" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/header_footer_login.css.xhtml?
```

```
ln=transglobe" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-
layout" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/components.css.xhtml?
ln=primefaces&amp;v=6.1" /><script type="text/javascript"
src="/cs/javax.faces.resource/jquery/jquery.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/core.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/components.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/jquery/jquery-plugins.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/primefaces-extensions.js.xhtml?ln=primefaces-
extensions&amp;v=6.1"></script><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/blockui/blockui.css.xhtml?ln=primefaces-
extensions&amp;v=6.1" /><script type="text/javascript"
src="/cs/javax.faces.resource/blockui/blockui.js.xhtml?ln=primefaces-
extensions&amp;v=6.1"></script><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/layout-blue.css.xhtml?ln=barcelona-
layout" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/ripple.css.xhtml?ln=barcelona-
layout" /><script type="text/javascript">if(window.PrimeFaces)
{PrimeFaces.settings.locale='zh_TW';}</script>

      <title> - (PCR-UAT)</title>
      <link rel="shortcut icon" type="image/x-icon"
href="/cs/javax.faces.resource/transglobe/img/logo.ico.xhtml" />


      <style id="antiClickjack">body{display:none !important;}
</style><script type="text/javascript"
src="/cs/javax.faces.resource/js/sas.js.xhtml?ln=barcelona-layout"></script>


      <script src="https://www.googletagmanager.com/gtag/js?id=UA-116871856-
1"></script>
      <script>
            window.dataLayer = window.dataLayer || [];
            function gtag() {
                  dataLayer.push(arguments);
            }
            gtag('js', new Date());

            gtag('config', 'UA-116871856-1');

            if (self === top) {
                var antiClickjack = document.getElementById
("antiClickjack");
                antiClickjack.parentNode.removeChild(antiClickjack);
            } else {
                top.location = self.location;
            }
      </script></head><body class="landing-body">

<div class="mask-content"></div>
<div class="globe-site">
      <div id="mainContent" class="layout-site-content login-template"><span
id="logonTop"><div id="j_idt12" class="ui-outputpanel ui-widget
maintain"><div class="ui-outputpanel-loading ui-widget"></div></div><script
id="j_idt12_s" type="text/javascript">$(function(

...TRUNCATED...
```

High Issues

Password Management: Weak Password Policy (11496) View Description

CWE: 521

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=userName2&javax.faces.partial.execute=userName2&javax.faces.partial.render=userName2&javax.faces.behavior.event=change&javax.faces.partial.event=change&form=form&userName2=H158462863&userPwd=&javax.faces.ViewState=4774089222092304441%3A-341459686818954549

Request:

```
POST /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Referer: https://uat2-eservice.transglobe.com.tw/cs/Logon/Logon.xhtml
Content-Length: 304
Pragma: no-cache
Cookie: JSESSIONID=qKVx1HRD3M6Z5WeFd314lMYQ; BIGipServerpool_UAT2-
ESERVICE=1799570186.9760.0000; _ga=GA1.3.1729844940.1553925630;
_gid=GA1.3.546018925.1553925630;
_gat_gtag_UA_116871856_1=1;CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2
788E4F20DA3E8FYB3BD
Connection: keep-alive
Pragma: no-cache
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Crawl.EventMacro.Startup";
SID="A73867865EB731AC65456598E455DED5"; SessionType="StartMacro";
CrawlType="None";
X-RequestManager-Memo: sid="29"; smi="0"; Category="EventMacro.Login";
MacroName="LoginMacro1";
X-Request-Memo: ID="93e46e8e-9f57-4f91-bd89-347660ac35ad"; tid="92";

javax.faces.partial.ajax=true&javax.faces.source=userName2&javax.faces.parti
al.execute=userName2&javax.faces.partial.render=userName2&javax.faces.behavi
or.event=change&javax.faces.partial.event=change&form=form&userName2=H158462
863&userPwd=&javax.faces.ViewState=4774089222092304441%3A-341459686818954549
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Content-Type: text/xml;charset=UTF-8
Content-Length: 729
Date: Sat, 30 Mar 2019 06:00:37 GMT

<?xml version='1.0' encoding='UTF-8'?>
<partial-response><changes><update id="userName2"><![CDATA[<input
id="userName2" name="userName2" type="text" value="H158462863"
maxlength="20" tabindex="1" title="" onchange="PrimeFaces.ab
({s:&quot;userName2&quot;,e:&quot;change&quot;,p:&quot;userName2&quot;,u:&qu
ot;userName2&quot;});" class="ui-inputfield ui-inputtext ui-widget ui-state-
default ui-corner-all" /><script id="userName2_s"
type="text/javascript">PrimeFaces.cw("InputText","widget_userName2",
{id:"userName2"});</script>]]></update><update id="javax.faces.ViewState"><!
[CDATA[4774089222092304441:-341459686818954549]]></update><eval><![CDATA[PF
('blockUIWidget').unblock();;]]></eval></changes></partial-response>
```

Medium Issues

Poor Error Handling: Unhandled Exception (1498) View Description

CWE: 388,497,200

Kingdom: Errors

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=userName2&javax.faces.partial.execute=userName2&javax.faces.partial.render=userName2&javax.faces.behavior.event=change&javax.faces.partial.event=change&form=form&userName2=H158462863&userPwd=&javax.faces.ViewState=%00

Request:

```
POST /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Referer: https://uat2-eservice.transglobe.com.tw/cs/Logon/Logon.xhtml
Content-Length: 266
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="DF790F45C8758ED1D32D33CFA56C7D41";
PSID="E585873D49E7F1B303FC2EED27E5AE89"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde";
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState";
AttackParamIndex="9"; AttackParamSubIndex="0"; CheckId="2134";
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="41";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="33"; smi="0"; sc="1"; ID="d7c734b6-5ccd-4d07-
9066-eb520919ab47";
X-Request-Memo: ID="7c291ab1-9cd4-4bb2-8c16-72fc34e9f2e3"; sc="1";
ThreadId="49";
Cookie: JSESSIONID=GyZE4lVTbO-cKyvA46uO3azk; BIGipServerpool_UAT2-
ESERVICE=960709386.9760.0000;CustomCookie=WebInspect121568ZX08AA2D62DE924F83
B2788E4F20DA3E8FYB3BD
Pragma: no-cache

...TRUNCATED...erName2=H158462863&userPwd=&javax.faces.ViewState=%00
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 1337
Date: Sat, 30 Mar 2019 06:05:16 GMT
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception
report</p><p><b>JBWEB000068: message</b> <u></u></p><p><...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml

PostData: j_idt54=j_idt54&javax.faces.ViewState=-1406235985234129637%3a7684428199681432905

Request:

```
POST /cs/errorpages/error.xhtml HTTP/1.1
Referer: https://uat2-eservice.transglobe.com.tw/cs/errorpages/error.xhtml
Content-Type: application/x-www-form-urlencoded
Content-Length: 80
Accept: */*
Pragma: no-cache
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Host: uat2-eservice.transglobe.com.tw
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="83DBA4B19979B1A6616B6F4A09EB4A8C";
PSID="78BD1F984019764588F66392943219C5"; SessionType="AuditAttack";
CrawlType="None"; AttackType="CookieParamManipulation";
OriginatingEngineID="90e84d4b-fe51-47a6-ace4-be01fbb9325c";
AttackSequence="0"; AttackParamDesc="_gat_gtag_UA_116871856_1";
AttackParamIndex="5"; AttackParamSubIndex="0"; CheckId="3582";
Engine="Http+Response+Splitting"; SmartMode="NonServerSpecificOnly";
AttackString="1%250d%250aSPIHeader%3a%2520SPIValue";
AttackStringProps="Attack"; ThreadId="35";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="49"; smi="0"; sc="1"; ID="d21a4628-ddb8-4898-
8fa8-5a7df0e7ba1c";
X-Request-Memo: ID="5c421601-889b-41bd-8d9c-ebb7320d2f0b"; sc="1";
ThreadId="57";
Cookie:
CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD;JSESSIO
NID=cmTRlHLkTlakRKnCkObMLmC1;BIGipServerpool_UAT2-
ESERVICE=960709386.9760.0000;_ga=GA1.2.1661686312.1553925942;_gid=GA1.2.9880
32260.1553925940;_gat_gtag_UA_116871856_1=1%0d%0aSPIHeader:%20SPIValue
;_ga=GA1.3.1661686312.1553925942;_gid=GA1.3.988032...TRUNCATED...
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 6782
Date: Sat, 30 Mar 2019 06:09:02 GMT
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception
report</p><p><b>JBWEB000068: message</b> <u></u></p><p><...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/Home/HomePage.xhtml

Request:

```
GET /cs/Main/Home/HomePage.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8%0d%
0aSPIHeader:%20SPIValue
Accept-Language: en-US,en;q=0.5
Accept-Encoding...TRUNCATED...
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
```

```
Content-Length: 7152
Date: Sat, 30 Mar 2019 06:04:49 GMT
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception
report</p><p><b>JBWEB000068: message</b> <u></u></p><p><...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml

PostData: j_idt54=http://www.webinspect.hp.com/&javax.faces.ViewState=-1406235985234129637%3a7684428199681432905

Request:

```
POST /cs/errorpages/error.xhtml HTTP/1.1
Referer: https://uat2-eservice.transglobe.com.tw/cs/errorpages/error.xhtml
Content-Type: application/x-www-form-urlencoded
Content-Length: 102
Accept: */*
Pragma: no-cache
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Host: uat2-eservice.transglobe.com.tw
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="73E0D78EB26E59589DF2AAEE14D7794E";
PSID="78BD1F984019764588F66392943219C5"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="e974f0fd-2e0a-4f6d-8ddc-95c224ed2191";
AttackSequence="0"; AttackParamDesc="j_idt54"; AttackParamIndex="0";
AttackParamSubIndex="0"; CheckId="10705";
Engine="Parameter+Based+Redirection"; SmartMode="NonServerSpecificOnly";
AttackString="http%3a%2f%2fwww.webinspect.hp.com%2f";
AttackStringProps="Attack"; ThreadId="35";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="49"; smi="0"; sc="1"; ID="1cfedc2b-aae2-4e84-
987d-e0228eceface";
X-Request-Memo: ID="28497bc8-2516-49e9-a87d-be712b7d387b"; sc="1";
ThreadId="57";
Cookie:
CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD;JSESSIO
NID=kqSt9FEi7lvZOIhwjChC4-EE;BIGipServerpool_UAT2-
ESERVICE=960709386.9760.0000;_ga=GA1.2.1661686312.1553925942;_gid=GA1.2.9880
32260.1553925940;_ga=GA1.3.1661686312.1553925942;_gid=GA1.3.988032260.155392
5940

j_idt54=http://www.webinspect.hp.com/
&javax.faces.ViewState=-1406235985234129637%3a7684...
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 6782
Date: Sat, 30 Mar 2019 06:09:02 GMT
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception
report</p><p><b>JBWEB000068: message</b> <u></u></p><p><...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=j_idt15%3Aj_idt18&javax.faces.partial.execute=%

40all&j_idt15%3Aj_idt18=j_idt15%3Aj_idt18&j_idt15=j_idt15&javax.faces.ViewState=%00

Request:

```
POST /cs/errorpages/error.xhtml HTTP/1.1
Referer: https://uat2-eservice.transglobe.com.tw/cs/errorpages/error.xhtml
Host: uat2-eservice.transglobe.com.tw
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Content-Length: 179
X-AscRawUrl: /cs/errorpages/error.xhtml
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="A360D2C92B273BCFBDC28955E047D367";
PSID="B0546A4ACCE1B0ACFE4B7808FE9B461D"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde";
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState";
AttackParamIndex="5"; AttackParamSubIndex="0"; CheckId="2134";
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="34";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="33"; smi="0"; sc="1"; ID="cd0a1d14-66f8-468e-
bc85-52b7680bebbd";
X-Request-Memo: ID="613ec456-b315-4425-8351-ac5d3e1602f8"; sc="1";
ThreadId="49";
Cookie:
CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD;JSESSIO
NID=YQuFcrhUVJM-QZw2cyTOrDbY;BIGipServerpool_UAT2-
ESERVICE=1799570186.9760.0000;_ga=GA1.2.1191292693.1553925940;_gid=GA1.2.752
867613.1553925940

...TRUNCATED...5%3Aj_idt18&j_idt15=j_idt15&javax.faces.ViewState=%00
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 6062
Date: Sat, 30 Mar 2019 06:08:40 GMT
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception
report</p><p><b>JBWEB000068: message</b> <u></u></p><p><...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml

PostData: j_idt54=j_idt54&javax.faces.ViewState=%00

Request:

```
POST /cs/errorpages/error.xhtml HTTP/1.1
Referer: https://uat2-eservice.transglobe.com.tw/cs/errorpages/error.xhtml
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Accept: */*
Pragma: no-cache
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
```

```
Firefox/30.0
Host: uat2-eservice.transglobe.com.tw
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="0E521C603EEF211E86FE005C5499E163";
PSID="78BD1F984019764588F66392943219C5"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde";
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState";
AttackParamIndex="1"; AttackParamSubIndex="0"; CheckId="2134";
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="35";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="49"; smi="0"; sc="1"; ID="8e730cf5-a451-4683-
a34d-51dcc4dc1e45";
X-Request-Memo: ID="6c707466-14ea-49ab-89ef-569aa8837562"; sc="1";
ThreadId="57";
Cookie:
CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD;JSESSIO
NID=kqSt9FEi7lvZOIhwjChC4-EE;BIGipServerpool_UAT2-
ESERVICE=960709386.9760.0000;_ga=GA1.2.1661686312.1553925942;_gid=GA1.2.9880
32260.1553925940;_ga=GA1.3.1661686312.1553925942;_gid=GA1.3.988032260.155392
5940

j_idt54=j_idt54&javax.faces.ViewState=^^
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 6131
Date: Sat, 30 Mar 2019 06:09:05 GMT
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception 
report</p><p><b>JBWEB000068: message</b> <u>String index...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=j_idt12&primefaces.ignoreautoupdate=true&javax.faces.partial.execute=j_idt12&javax.faces.partial.render=j_idt12&j_idt12=j_idt12&j_idt12_load=true&form=form&userName2=&userPwd=&javax.faces.ViewState=%00

Request:

```
POST /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Referer: https://uat2-eservice.transglobe.com.tw/cs/Logon/Logon.xhtml
Content-Length: 250
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="136FC185DECA67D8F1A136DF67CD45BF";
PSID="E1446B115B5E82DFE28BF67B52C84002"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde";
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState";
```

```
AttackParamIndex="10"; AttackParamSubIndex="0"; CheckId="2134";
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="36";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="47"; smi="0"; sc="1"; ID="83658607-6f60-4bc3-
a14f-2edf7f177253";
X-Request-Memo: ID="2af4a679-3086-4399-8af6-bf618e3978fe"; sc="1";
ThreadId="56";
Cookie: JSESSIONID=HALuxqiukNbmiw7Nt-QhNPUr; BIGipServerpool_UAT2-
ESERVICE=960709386.9760.0000;CustomCookie=WebInspect121568ZX08AA2D62DE924F83
B2788E4F20DA3E8FYB3BD
Pragma: no-cache

...TRUNCATED...rm=form&userName2=&userPwd=&javax.faces.ViewState=%00
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 1337
Date: Sat, 30 Mar 2019 06:05:18 GMT
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception
report</p><p><b>JBWEB000068: message</b> <u></u></p><p><...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=j_idt15%3Aj_idt18&javax.faces.partial.execute=%40all&j_idt15%3Aj_idt18=j_idt15%3Aj_idt18&j_idt15=j_idt15&javax.faces.ViewState=%00

Request:

```
POST /cs/Main/OwnerArea/OwnerHeartTip.xhtml HTTP/1.1
Referer: https://uat2-
eservice.transglobe.com.tw/cs/Main/OwnerArea/OwnerHeartTip.xhtml
Host: uat2-eservice.transglobe.com.tw
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Content-Length: 179
X-AscRawUrl: /cs/Main/OwnerArea/OwnerHeartTip.xhtml
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="20F18297813254A5C34A997671F3EE50";
PSID="A81CE5630FD0DF1F787EBA581D0FF37B"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde";
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState";
AttackParamIndex="5"; AttackParamSubIndex="0"; CheckId="2134";
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="36";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="43"; smi="0"; sc="1"; ID="e6276ac2-5aec-4f85-
b234-f1f35cae4398";
X-Request-Memo: ID="717eba6e-bc50-4116-b3b4-c42ecb383bfd"; sc="1";
ThreadId="54";
Cookie:
CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD;JSESSIO
```

```
NID=qKVx1HRD3M6Z5WeFd314lMYQ;BIGipServerpool_UAT2-
ESERVICE=1799570186.9760.0000;_ga=GA1.2.421486780.1553925884;_gid=GA1.2.1352
871653.1553925884

...TRUNCATED...5%3Aj_idt18&j_idt15=j_idt15&javax.faces.ViewState=%00
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 6139
Date: Sat, 30 Mar 2019 06:08:36 GMT
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception 
report</p><p><b>JBWEB000068: message</b> <u></u></p><p><...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=logonBtn&javax.faces.partial.execute=%40all&javax.faces.partial.render=form&logonBtn=logonBtn&form=form&userName2=H158462863&userPwd=123456&javax.faces.ViewState=%00

Request:

```
POST /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 
Firefox/30.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Referer: https://uat2-eservice.transglobe.com.tw/cs/Logon/Logon.xhtml
Content-Length: 214
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack"; 
SID="43D4C85F88E08196470A002A1B3869A7"; 
PSID="46C660C73B9E54D7F02900F25E180C61"; SessionType="AuditAttack"; 
CrawlType="None"; AttackType="PostParamManipulation"; 
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde"; 
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState"; 
AttackParamIndex="8"; AttackParamSubIndex="0"; CheckId="2134"; 
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="40"; 
ThreadType="AuditorStateRequestorPool"; 
X-RequestManager-Memo: sid="33"; smi="0"; sc="1"; ID="c2a2bed5-deda-46a1-
bfa2-2c4eb7b8736d";
X-Request-Memo: ID="8f80cfe9-8004-45d4-93bd-61d195025dd5"; sc="1"; 
ThreadId="49";
Cookie: JSESSIONID=GyZE4lVTbO-cKyvA46uO3azk; BIGipServerpool_UAT2-
ESERVICE=960709386.9760.0000;CustomCookie=WebInspect121568ZX08AA2D62DE924F83
B2788E4F20DA3E8FYB3BD
Pragma: no-cache

...TRUNCATED...2=H158462863&userPwd=123456&javax.faces.ViewState=%00
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Length: 1337
Date: Sat, 30 Mar 2019 06:05:15 GMT
```

```
Connection: close

...TRUNCATED...noshade"><p><b>JBWEB000309: type</b> JBWEB000066: Exception 
report</p><p><b>JBWEB000068: message</b> <u></u></p><p><...TRUNCATED...
```

Cookie Security: Cookie Not Sent Over SSL (4720) View Description

CWE: 614

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Request:

```
GET /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 
Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Crawl.EventMacro.Startup"; 
SID="BCEAF30F249217B459AC90AFE417D8DC"; SessionType="StartMacro"; 
CrawlType="None";
X-RequestManager-Memo: sid="29"; smi="0"; Category="EventMacro.Login"; 
MacroName="LoginMacro1";
X-Request-Memo: ID="4a97cb7d-22fd-444e-8c43-67f52f82eb8a"; tid="81";
Pragma: no-cache
Cookie: CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Length: 14766
Set-Cookie: JSESSIONID=qKVx1HRD3M6Z5WeFd314lMYQ; Path=/cs; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
Date: Sat, 30 Mar 2019 06:00:30 GMT
Set-Cookie: BIGipServerpool_UAT2-ESERVICE=1799570186.9760.0000; path=/

<!DOCTYPE html>
<html xmlns="http://www.w3.org...TRUNCATED...
```

Cross-Frame Scripting (11294) View Description

CWE: 352

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerHeartTip.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 
Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

```
Referer: https://uat2-eservice.transglobe.com.tw/cs/Logon/Logon.xhtml
Pragma: no-cache
Cookie: JSESSIONID=qKVx1HRD3M6Z5WeFd314lMYQ; BIGipServerpool_UAT2-
ESERVICE=1799570186.9760.0000; _ga=GA1.3.1729844940.1553925630;
_gid=GA1.3.546018925.1553925630;
_gat_gtag_UA_116871856_1=1;CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2
788E4F20DA3E8FYB3BD
Connection: keep-alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Crawl.EventMacro.Startup";
SID="C9F867A9487A9F237DC76F9BE12F3D2B"; SessionType="StartMacro";
CrawlType="None";
X-RequestManager-Memo: sid="29"; smi="0"; Category="EventMacro.Login";
MacroName="LoginMacro1";
X-Request-Memo: ID="f3b26ad8-b776-41ed-97c7-13fd715a6525"; tid="92";
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Date: Sat, 30 Mar 2019 06:01:38 GMT
Content-Length: 31372

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml"><head id="j_idt2">
            <meta http-equiv="X-UA-Compatible" content="IE=edge" />
            <meta http-equiv="Content-Type" content="text/html; charset=UTF-
8" />
            <meta name="viewport" content="width=device-width, initial-
scale=1.0, maximum-scale=1.0, user-scalable=0" />

            <meta name="apple-mobile-web-app-capable" content="yes" /><link
type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/theme.css.xhtml?ln=primefaces-barcelona-
blue" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/fa/font-awesome.css.xhtml?
ln=primefaces&amp;v=6.1" /><script type="text/javascript"
src="/cs/javax.faces.resource/jquery/jquery.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/core.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/idlemonitor/idlemonitor.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/jquery/jquery-plugins.js.xhtml?
ln=primefaces&amp;v=6.1"></script><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/components.css.xhtml?
ln=primefaces&amp;v=6.1" /><script type="text/javascript"
src="/cs/javax.faces.resource/components.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/primefaces-extensions.js.xhtml?ln=primefaces-
extensions&amp;v=6.1"></script><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/blockui/blockui.css.xhtml?ln=primefaces-
extensions&amp;v=6.1" /><script type="text/javascript"
src="/cs/javax.faces.resource/blockui/blockui.js.xhtml?ln=primefaces-
extensions&amp;v=6.1"></script><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/header_footer_MainSouth.css.xhtml?
ln=transglobe" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/nanoscroller.css.xhtml?ln=barcelona-
layout" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/animate.css.xhtml?ln=barcelona-
layout" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/ripple.css.xhtml?ln=barcelona-
layout" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/layout-blue.css.xhtml?ln=barcelona-
layout" /><script type="text/javascript">if(win
dow.PrimeFaces){PrimeFaces.settings.locale='zh_TW';}</script>
```

```
    <title> - (PCR-UAT)</title>

      <link rel="shortcut icon" type="image/x-icon"
href="/cs/javax.faces.resource/barcelona-
layout/images/favicon.ico.xhtml" /><script type="text/javascript"
src="/cs/javax.faces.resource/js/nanoscroller.js.xhtml?ln=barcelona-
layout"></script><script type="text/javascript"
src="/cs/javax.faces.resource/js/layout.js.xhtml?ln=barcelona-
layout"></script><script type="text/javascript"
src="/cs/javax.faces.resource/js/ripple.js.xhtml?ln=barcelona-
layout"></script><script type="text/javascript"
src="/cs/javax.faces.resource/js/localzhTW.js.xhtml?ln=barcelona-
layout"></script><script type="text/javascript"
src="/cs/javax.faces.resource/js/jquery-ui.js.xhtml?ln=barcelona-
layout"></script><script type="text/javascript"
src="/cs/javax.faces.resource/js/JQueryDatePickerTW.js.xhtml?ln=barcelona-
layout"></script><script type="text/javascript"
src="/cs/javax.faces.resource/js/sas.js.xhtml?ln=barcelona-layout"></script>


      <script src="https://www.googletagmanager.com/gtag/js?id=UA-116871856-
1"></script>
      <script>
            window.dataLayer = window.dataLayer || [];
            function gtag(){dataLayer.push(arguments);}
            gtag('js', new Date());

            gtag('config', 'UA-116871856-1');
      </script>

      <style id="antiClickjack">body{display:none !important;}</style>
      <style>
            .scrollup {
                  width: 64px;
                  height: 63px;
                  position: fixed;
                  bottom: 100px;
                  right: 100px;
                  display: none;
                  text-indent: -9999px;
                  background-image: url('/cs/resources/barcelo

...TRUNCATED...
```

Privacy Violation: Inconsistent Feedback (11418) View Description

CWE: 209

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=userName2&javax.faces.partial.execute=userName2&javax.faces.partial.render=userName2&javax.faces.behavior.event=change&javax.faces.partial.event=change&form=form&userName2=spiuser&userPwd=&javax.faces.ViewState=4315725940006186430%3A3657088062404899036

Request:

```
POST /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
```

```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Referer: https://uat2-eservice.transglobe.com.tw/cs/Logon/Logon.xhtml
Content-Length: 301
Pragma: no-cache
Cookie: JSESSIONID=1HIgY-CRTAtWK2a4QblqNXX4; BIGipServerpool_UAT2-
ESERVICE=1799570186.9760.0000; _ga=GA1.3.1856925090.1553925903;
_gid=GA1.3.582059756.1553925903;
_gat_gtag_UA_116871856_1=1;CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2
788E4F20DA3E8FYB3BD
Connection: keep-alive
Pragma: no-cache
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.EventMacro.Workflow";
SID="90DF5137F3AC9D5A0AA4DD9101AA636A"; SessionType="NamedMacro";
CrawlType="None"; OriginatingEngineID="41d8521e-1c73-444b-80fa-
3518246dca05"; TriggerSID="E585873D49E7F1B303FC2EED27E5AE89";
X-RequestManager-Memo: sid="95"; smi="0"; Category="EventMacro.Named";
MacroName="none";
X-Request-Memo: ID="3b64191c-5aa0-4e21-abe5-fb29c6f9317d"; tid="182";

...TRUNCATED...ax.faces.partial.event=change&form=form&userName2=spiuser
&userPwd=&javax.faces.ViewState=431572594000618643...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache
Content-Type: text/xml;charset=UTF-8
Content-Length: 726
Date: Sat, 30 Mar 2019 06:05:09 GMT
```

Insecure Transport: Weak SSL Protocol (11516)

View Description

CWE: 327

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Request:

```
GET /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Crawl.EventMacro.Startup";
SID="BCEAF30F249217B459AC90AFE417D8DC"; SessionType="StartMacro";
CrawlType="None";
X-RequestManager-Memo: sid="29"; smi="0"; Category="EventMacro.Login";
MacroName="LoginMacro1";
X-Request-Memo: ID="4a97cb7d-22fd-444e-8c43-67f52f82eb8a"; tid="81";
Pragma: no-cache
Cookie: CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Length: 14766
Set-Cookie: JSESSIONID=qKVx1HRD3M6Z5WeFd314lMYQ; Path=/cs; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
Date: Sat, 30 Mar 2019 06:00:30 GMT
Set-Cookie: BIGipServerpool_UAT2-ESERVICE=1799570186.9760.0000; path=/

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml"><head id="j_idt2">
      <meta http-equiv="X-UA-Compatible" content="IE=9; IE=EDGE" />
      <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
            <meta http-equiv="Content-Type" content="text/html; charset=UTF-
8" />
            <meta http-equiv="refresh" content="300" />
            <meta name="viewport" content="width=device-width, initial-
scale=1.0, maximum-scale=1.0, user-scalable=yes" />
            <meta name="format-detection" content="telephone=no" />
            <meta name="apple-mobile-web-app-capable" content="yes" />
            <meta name="apple-mobile-web-app-status-bar-style"
content="black" />
            <meta name="keywords" content=", , ,
, , " /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/theme.css.xhtml?ln=primefaces-barcelona-
blue" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/fa/font-awesome.css.xhtml?
ln=primefaces&amp;v=6.1" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/layout-login.css.xhtml?
ln=transglobe" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/header_footer_login.css.xhtml?
ln=transglobe" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-
layout" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/components.css.xhtml?
ln=primefaces&amp;v=6.1" /><script type="text/javascript"
src="/cs/javax.faces.resource/jquery/jquery.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/core.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/components.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/jquery/jquery-plugins.js.xhtml?
ln=primefaces&amp;v=6.1"></script><script type="text/javascript"
src="/cs/javax.faces.resource/primefaces-extensions.js.xhtml?ln=primefaces-
extensions&amp;v=6.1"></script><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/blockui/blockui.css.xhtml?ln=primefaces-
extensions&amp;v=6.1" /><script type="text/javascript"
src="/cs/javax.faces.resource/blockui/blockui.js.xhtml?ln=primefaces-
extensions&amp;v=6.1"></script><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/layout-blue.css.xhtml?ln=barcelona-
layout" /><link type="text/css" rel="stylesheet"
href="/cs/javax.faces.resource/css/ripple.css.xhtml?ln=barcelona-
layout" /><script type="text/javascript">if(window.PrimeFaces)
{PrimeFaces.settings.locale='zh_TW';}</script>

      <title> - (PCR-UAT)</title>
      <link rel="shortcut icon" type="image/x-icon"
href="/cs/javax.faces.resource/transglobe/img/logo.ico.xhtml" />


      <style id="antiClickjack">body{display:none !important;}
</style><script type="text/javascript"
src="/cs/javax.faces.resource/js/sas.js.xhtml?ln=barcelona-layout"></script>


      <script src="https://www.googletagmanager.com/gtag/js?id=UA-116871856-
1"></script>
```

```
      <script>
            window.dataLayer = window.dataLayer || [];
            function gtag() {
                  dataLayer.push(arguments);
            }
            gtag('js', new Date());

            gtag('config', 'UA-116871856-1');

            if (self === top) {
                var antiClickjack = document.getElementById
("antiClickjack");
                antiClickjack.parentNode.removeChild(antiClickjack);
            } else {
                top.location = self.location;
            }
      </script></head><body class="landing-body">

<div class="mask-content"></div>
<div class="globe-site">
      <div id="mainContent" class="layout-site-content login-template"><span
id="logonTop"><div id="j_idt12" class="ui-outputpanel ui-widget
maintain"><div class="ui-outputpanel-loading ui-widget"></div></div><script
id="j_idt12_s" type="text/javascript">$(function(

...TRUNCATED...
```

Low Issues

Cookie Security: HTTPOnly not Set (10543) View Description

CWE: 284

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Request:

```
GET /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Crawl.EventMacro.Startup";
SID="BCEAF30F249217B459AC90AFE417D8DC"; SessionType="StartMacro";
CrawlType="None";
X-RequestManager-Memo: sid="29"; smi="0"; Category="EventMacro.Login";
MacroName="LoginMacro1";
X-Request-Memo: ID="4a97cb7d-22fd-444e-8c43-67f52f82eb8a"; tid="81";
Pragma: no-cache
Cookie: CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Length: 14766
Set-Cookie: JSESSIONID=qKVx1HRD3M6Z5WeFd314lMYQ; Path=/cs; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
```

```
Date: Sat, 30 Mar 2019 06:00:30 GMT
Set-Cookie: BIGipServerpool_UAT2-ESERVICE=1799570186.9760.0000; path=/

<!DOCTYPE html>
<html xmlns="http://www.w3.org...TRUNCATED...
```

Web Server Misconfiguration: Server Error Message (10932)

View Description

CWE: 388,497,200

Kingdom: Environment

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=logonBtn&javax.faces.partial.execute=%40all&javax.faces.partial.render=form&logonBtn=logonBtn&form=form&userName2=H158462863&userPwd=123456&javax.faces.ViewState=%00

Request:

```
POST /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Referer: https://uat2-eservice.transglobe.com.tw/cs/Logon/Logon.xhtml
Content-Length: 214
Pragma: no-cache
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="43D4C85F88E08196470A002A1B3869A7";
PSID="46C660C73B9E54D7F02900F25E180C61"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde";
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState";
AttackParamIndex="8"; AttackParamSubIndex="0"; CheckId="2134";
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="40";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="33"; smi="0"; sc="1"; ID="c2a2bed5-deda-46a1-
bfa2-2c4eb7b8736d";
X-Request-Memo: ID="8f80cfe9-8004-45d4-93bd-61d195025dd5"; sc="1";
ThreadId="49";
Cookie: JSESSIONID=GyZE41VTbO-cKyvA46uO3azk; BIGipServerpool_UAT2-
ESERVICE=960709386.9760.0000;CustomCookie=WebInspect121568ZX08AA2D62DE924F83
B2788E4F20DA3E8FYB3BD
Pragma: no-cache

...TRUNCATED...2=H158462863&userPwd=123456&javax.faces.ViewState=%00
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml

PostData: j_idt47=j_idt47&javax.faces.ViewState=%00

Request:

```
POST /cs/Main/OwnerArea/OwnerHeartTip.xhtml HTTP/1.1
Referer: https://uat2-
eservice.transglobe.com.tw/cs/Main/OwnerArea/OwnerHeartTip.xhtml
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Accept: */*
Pragma: no-cache
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Host: uat2-eservice.transglobe.com.tw
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="9250FB7834DE160290307F1FF457B682";
PSID="BB6D14FAF5B78868A967672E345B2FD7"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde";
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState";
AttackParamIndex="1"; AttackParamSubIndex="0"; CheckId="2134";
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="37";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="47"; smi="0"; sc="1"; ID="543a3233-cffe-44b1-
9582-2987eae8eac4";
X-Request-Memo: ID="1994f6bd-2a8c-43b1-8b87-347986888f0b"; sc="1";
ThreadId="56";
Cookie:
CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD;JSESSIO
NID=qKVx1HRD3M6Z5WeFd314lMYQ;BIGipServerpool_UAT2-
ESERVICE=1799570186.9760.0000;_ga=GA1.2.713716651.1553925971;_gid=GA1.2.1123
644494.1553925971

j_idt47=j_idt47&javax.faces.ViewState=^^
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/<script>alert('TRACK');</script>

Request:

```
TRACK /<script>alert('TRACK');</script> HTTP/1.1
Referer: https://uat2-
eservice.transglobe.com.tw/cs/javax.faces.resource/css/layout-
login.css.xhtml?ln=transglobe
Accept: */*
Pragma: no-cache
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Host: uat2-eservice.transglobe.com.tw
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="699154B4631C8511ABC244AF66E15AA2";
PSID="7A0F34EC76A2FAC2D025B6F7E83E82D4"; SessionType="AuditAttack";
CrawlType="None"; AttackType="Search"; OriginatingEngineID="65cee7d3-561f-
40dc-b5eb-c0b8c2383fcb"; AttackSequence="0"; AttackParamDesc="";
AttackParamIndex="0"; AttackParamSubIndex="0"; CheckId="5152";
Engine="Request+Modify"; SmartMode="NonServerSpecificOnly"; ThreadId="36";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="45"; smi="0"; sc="1"; ID="36112140-6366-4a51-
878c-a2a6370355a0";
X-Request-Memo: ID="4986da01-ff46-4eba-b598-e833001ce280"; sc="1";
```

```
ThreadId="55";
Cookie:
CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD;BIGipSe
rverpool_UAT2-ESERVICE=960709386.9760.0000
```

Response:

```
HTTP/1.1 501 Not Implemented
Server: Apache-Coyote/1.1
Conte...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml

PostData: javax.faces.partial.ajax=true&javax.faces.source=j_idt15%3Aj_idt18&javax.faces.partial.execute=%40all&j_idt15%3Aj_idt18=j_idt15%3Aj_idt18&j_idt15=j_idt15&javax.faces.ViewState=%00

Request:

```
POST /cs/errorpages/error.xhtml HTTP/1.1
Referer: https://uat2-eservice.transglobe.com.tw/cs/errorpages/error.xhtml
Host: uat2-eservice.transglobe.com.tw
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Faces-Request: partial/ajax
X-Requested-With: XMLHttpRequest
Content-Length: 179
X-AscRawUrl: /cs/errorpages/error.xhtml
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Connection: Keep-Alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Audit.Attack";
SID="A360D2C92B273BCFBDC28955E047D367";
PSID="B0546A4ACCE1B0ACFE4B7808FE9B461D"; SessionType="AuditAttack";
CrawlType="None"; AttackType="PostParamManipulation";
OriginatingEngineID="18264a0f-d83e-4ef5-a73d-1f06044c9fde";
AttackSequence="0"; AttackParamDesc="javax.faces.ViewState";
AttackParamIndex="5"; AttackParamSubIndex="0"; CheckId="2134";
Engine="Post+Injection"; SmartMode="NonServerSpecificOnly"; AttackString="%
2500"; AttackStringProps="Attack"; ThreadId="34";
ThreadType="AuditorStateRequestorPool";
X-RequestManager-Memo: sid="33"; smi="0"; sc="1"; ID="cd0a1d14-66f8-468e-
bc85-52b7680bebbd";
X-Request-Memo: ID="613ec456-b315-4425-8351-ac5d3e1602f8"; sc="1";
ThreadId="49";
Cookie:
CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD;JSESSIO
NID=YQuFcrhUVJM-QZw2cyTOrDbY;BIGipServerpool_UAT2-
ESERVICE=1799570186.9760.0000;_ga=GA1.2.1191292693.1553925940;_gid=GA1.2.752
867613.1553925940

...TRUNCATED...5%3Aj_idt18&j_idt15=j_idt15&javax.faces.ViewState=%00
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/Home/HomePage.xhtml

Request:

```
GET /cs/Main/Home/HomePage.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8%0d%
0aSPIHeader:%20SPIValue
Accept-Language: en-US,en;q=0.5
Accept-Encoding...TRUNCATED...
```

Response:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1...TRUNCATED...
```

Privacy Violation: Autocomplete (11276)

View Description

CWE: 200

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Request:

```
GET /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Crawl.EventMacro.Startup";
SID="BCEAF30F249217B459AC90AFE417D8DC"; SessionType="StartMacro";
CrawlType="None";
X-RequestManager-Memo: sid="29"; smi="0"; Category="EventMacro.Login";
MacroName="LoginMacro1";
X-Request-Memo: ID="4a97cb7d-22fd-444e-8c43-67f52f82eb8a"; tid="81";
Pragma: no-cache
Cookie: CustomCookie=WebInspect121568ZX08AA2D62DE924F83B2788E4F20DA3E8FYB3BD
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Content-Length: 14766
Set-Cookie: JSESSIONID=qKVx1HRD3M6Z5WeFd314lMYQ; Path=/cs; Secure; HttpOnly
Content-Type: text/html;charset=UTF-8
Date: Sat, 30 Mar 2019 06:00:30 GMT
Set-Cookie: BIGipServerpool_UAT2-ESERVICE=1799570186.9760.0000; path=/

...TRUNCATED... "></div>
                <div class="input-block"><input id="userPwd"
name="userPwd" type="password" class="ui-inputfield ui-password ui-widget ui
-state-default ui-corner-all" tabindex="2" /><script id="userPwd_s"
type="text/javascript">$(fu...TRUNCATED...
```

Cache Management: Insecure Policy (11306)

View Description

CWE: 525

Kingdom: Environment

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerBankAccountSetting.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerBankAccountSetting.xhtml HT...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/jquery/jquery-plugins.js.xhtml?ln=primefaces&v=6.1

Request:

```
GET /cs/javax.faces.resource/jquery/jquery-plugins.js.x...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/fonts/MaterialIcons-Regular.woff.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/fonts/MaterialIcons-Regula...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPolicyChangeNotice.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerPolicyChangeNotice.xhtml HT...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/css/msg.css.xhtml?ln=barce...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/primefaces-extensions.js.xhtml?

ln=primefaces-extensions&v=6.1

Request:

```
GET /cs/javax.faces.resource/primefaces-extensions.js.x...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/blockui/blockui.css.xhtml?ln=primefaces-extensions&v=6.1

Request:

```
GET /cs/javax.faces.resource/blockui/blockui.css.xhtml?...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/layout.js.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/js/layout.js.xhtml?ln=barc...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPolicyList.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerPolicyList.xhtml HTTP/1.1
...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerCreditCardMaintain.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerCreditCardMaintain.xhtml HT...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/sas.js.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/js/sas.js.xhtml?ln=barcelo...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerIncomeTax.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerIncomeTax.xhtml HTTP/1.1
R...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/core.js.xhtml?ln=primefaces&v=6.1

Request:

```
GET /cs/javax.faces.resource/core.js.xhtml?ln=primeface...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/transglobe/img/logo.ico.xhtml

Request:

```
GET /cs/javax.faces.resource/transglobe/img/logo.ico.xh...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerClaimsRecordQuery.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerClaimsRecordQuery.xhtml HTT...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/barcelona-layout/images/favicon.ico.xhtml

Request:

```
GET /cs/javax.faces.resource/barcelona-layout/images/fa...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/fa/fontawesome-webfont.ttf.xhtml?ln=primefaces&v=6.1?v=4.7.0

Request:

```
GET /cs/javax.faces.resource/fa/fontawesome-webfont.ttf...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerECServiceOpen.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerECServiceOpen.xhtml HTTP/1....TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/Home/HomePage.xhtml

Request:

```
GET /cs/Main/Home/HomePage.xhtml HTTP/1.1
Host: uat2-e...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/exception-style.css.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/css/exception-style.css.xh...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/nanoscroller.js.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/js/nanoscroller.js.xhtml?l...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
```

```
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerLoanRecordQuery.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerLoanRecordQuery.xhtml HTTP/...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/nanoscroller.css.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/css/nanoscroller.css.xhtml...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/animate.css.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/css/animate.css.xhtml?ln=b...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPayment.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerPayment.xhtml HTTP/1.1
Ref...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerContractChangeQuery.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerContractChangeQuery.xhtml H...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerOnlinePay01.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerOnlinePay01.xhtml HTTP/1.1...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/layout-login.css.xhtml?ln=transglobe

Request:

```
GET /cs/javax.faces.resource/css/layout-login.css.xhtml...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/idlemonitor/idlemonitor.js.xhtml?ln=primefaces&v=6.1

Request:

```
GET /cs/javax.faces.resource/idlemonitor/idlemonitor.js...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/components.js.xhtml?ln=primefaces&v=6.1

Request:

```
GET /cs/javax.faces.resource/components.js.xhtml?ln=pri...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/fa/fontawesome-webfont.woff.xhtml?ln=primefaces&v=6.1?v=4.7.0

Request:

```
GET /cs/javax.faces.resource/fa/fontawesome-webfont.wof...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPolicyChangeAndElectronicNotice.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerPolicyChangeAndElectronicNo...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/JQueryDatePickerTW.js.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/js/JQueryDatePickerTW.js.x...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/blockui/blockui.js.xhtml?ln=primefaces-extensions&v=6.1

Request:

```
GET /cs/javax.faces.resource/blockui/blockui.js.xhtml?l...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/ripple.css.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/css/ripple.css.xhtml?ln=ba...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/jquery/jquery.js.xhtml?ln=primefaces&v=6.1

Request:

```
GET /cs/javax.faces.resource/jquery/jquery.js.xhtml?ln=...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerPolicyCertificationServer.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerPolicyCertificationServer.x...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/jquery-ui.js.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/js/jquery-ui.js.xhtml?ln=b...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/header_footer_login.css.xhtml?ln=transglobe

Request:

```
GET /cs/javax.faces.resource/css/header_footer_login.cs...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/ripple.js.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/js/ripple.js.xhtml?ln=barc...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/js/localzhTW.js.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/js/localzhTW.js.xhtml?ln=b...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/layout-blue.css.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/css/layout-blue.css.xhtml?...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/errorpages/error.xhtml

Request:

```
GET /cs/errorpages/error.xhtml HTTP/1.1
Referer: https...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/Home/ChangPwd.xhtml

Request:

```
GET /cs/Main/Home/ChangPwd.xhtml HTTP/1.1
Referer: htt...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/theme.css.xhtml?ln=primefaces-barcelona-blue

Request:

```
GET /cs/javax.faces.resource/theme.css.xhtml?ln=primefa...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/header_footer_MainSouth.css.xhtml?ln=transglobe

Request:

```
GET /cs/javax.faces.resource/css/header_footer_MainSout...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml

Request:

```
GET /cs/Main/OwnerArea/OwnerHeartTip.xhtml HTTP/1.1
Ho...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/fa/font-awesome.css.xhtml?ln=primefaces&v=6.1

Request:

```
GET /cs/javax.faces.resource/fa/font-awesome.css.xhtml?...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/components.css.xhtml?ln=primefaces&v=6.1

Request:

```
GET /cs/javax.faces.resource/components.css.xhtml?ln=pr...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Page: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml

Request:

```
GET /cs/Logon/Logon.xhtml HTTP/1.1
Host: uat2-eservice...TRUNCATED...
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Opt...TRUNCATED...
```

Insecure Transport: HSTS Not Set (11365)

View Description

CWE: 319

Kingdom: Security Features

Page: https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-layout

Request:

```
GET /cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-layout HTTP/1.1
Host: uat2-eservice.transglobe.com.tw
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101
Firefox/30.0
Accept: text/css,*/*;q=0.1
```

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://uat2-eservice.transglobe.com.tw/cs/Logon/Logon.xhtml
Pragma: no-cache
Cookie: JSESSIONID=qKVx1HRD3M6Z5WeFd314lMYQ; BIGipServerpool_UAT2-
ESERVICE=1799570186.9760.0000;CustomCookie=WebInspect121568ZX08AA2D62DE924F8
3B2788E4F20DA3E8FYB3BD
Connection: keep-alive
X-WIPP: AscVersion=17.10.283.0
X-Scan-Memo: Category="Crawl.EventMacro.Startup";
SID="EABCBA0EAC49A6A8DE00641B7EA5C5B0"; SessionType="StartMacro";
CrawlType="None";
X-RequestManager-Memo: sid="29"; smi="0"; Category="EventMacro.Login";
MacroName="LoginMacro1";
X-Request-Memo: ID="6585e181-6075-4442-941a-187150377831"; tid="92";
```

Response:

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Frame-Options: SAMEORIGIN
Expires: Sat, 06 Apr 2019 06:00:30 GMT
Last-Modified: Mon, 25 Mar 2019 09:15:32 GMT
ETag: W/"263-1553505332000"
Content-Type: text/css;charset=UTF-8
Content-Length: 263
Date: Sat, 30 Mar 2019 06:00:30 GMT

.maintain {
      background: #EEF3F9;
      padding: .8em;
      margin: auto;
      line-height: 18px;
}

@media only screen and (min-width:480px) {
      .maintain {
            background: #EEF3F9;
            padding: .8em;
            margin: auto;
            padding-left: 20%;
            line-height: 18px;
      }
}
```

Appendix (Check Descriptions)

Insecure Transport: Weak SSL Cipher (11285)

Summary

WebInspect has detected support for weak TLS/SSL ciphers on server **https://uat2-eservice.transglobe.com.tw:443/** .

The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols provide a mechanism to help protect authenticity, confidentiality and integrity of the data transmitted between a client and web server. The strength of this protection mechanism is determined by the authentication, encryption and hashing algorithms, collectively known as a cipher suite, chosen for the transmission of sensitive information over the TLS/SSL channel. Most Web servers support a range of such cipher suites of varying strengths. Using a weak cipher or an encryption key of insufficient length, for example, could allow an attacker to defeat the protection mechanism and steal or modify sensitive information.

If misconfigured, a web server could be manipulated into choosing weak cipher suites. Recommendations include updating the web server configuration to always choose the strongest ciphers for encryption.

Execution

Each weak cipher was enumerated by establishing an SSL connection with the target host and specifying the cipher to test in the Client Hello message of the SSL handshake.

Implication

A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current methods and resources. An attacker may be able to execute a man-in-the-middle attack which would allow them to intercept, monitor and tamper with sensitive data.

Fix

Disable support for weak ciphers on the server. Weak ciphers are generally defined as:

- Any cipher with key length less than 128 bits
- Export-class cipher suites
- NULL ciphers
- Ciphers that support unauthenticated modes
- Ciphers assessed at security strenghts below 112 bits
- All RC4 ciphers
- All 64-bit block ciphers

The following ciphers supported by the server are weak and should be disabled:

- **TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)**

The weak cipher list above also includes ciphers that enable conditions for SWEET32 cipher attacks. The vulnerability affects all 64-bit block ciphers such as 3DES and Blowfish. The vulnerability is independent of the number of keys and/or the key length used in the cipher. It could allow attackers to obtain cleartext data from long-lived encrypted sessions. The vulnerability is identified by CVE-2016-2183 and CVE-2016-6329.

The following 64-bit block ciphers should be removed from the target server configuration to prevent SWEET32 attacks:

- **TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)**

- For Apache, modify the following lines in httpd.conf or ssl.conf:

- SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!NULL:!RC4:!RC2:!DES:!3DES+HIGH:+MEDIUM

- For IIS, please refer to Microsoft Knowledge Base Articles:

- Article ID: 187498
- Article ID: 245030 and
- Security Guidance for IIS
- Article ID: 2868725

- For other servers, please refer to vendor specific documentation.

The following ciphers supported by the server should provide adequate protection and may be left enabled:

- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)**

- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)**
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)**
- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)**
- **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)**
- **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)**

Reference

OWASP:
Transport Layer Protection Cheat Sheet

PCI Security Standards Council:
PCI DSS v3.1

CVE
CVE-2013-2566
CVE-2016-2183
CVE-2016-6329

NIST
NIST Special Publication 800-131A

Microsoft:
Knowledge Base Article ID: 2868725
Knowledge Base Article ID: 187498
Knowledge Base Article ID: 245030
Security Guidance for IIS

Apache:
SSL/TLS Strong Encryption: FAQ

RC4:
New RC4 Attack

ACM CCS '16
On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN

Classifications

CWE-319: Cleartext Transmission of Sensitive Information
http://cwe.mitre.org/data/definitions/319.html

CWE-326: Inadequate Encryption Strength
http://cwe.mitre.org/data/definitions/326.html

CWE-327: Use of a Broken or Risky Cryptographic Algorithm
http://cwe.mitre.org/data/definitions/327.html

Kingdom: Security Features
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Password Management: Weak Password Policy (11496)

Summary

Authentication is an important aspect of security. Password authentication requires users to present login credentials as evidence to validate their identity before granting them access to server resources. The reliability of the authentication process depends on the security of the login credentials. Password policies that ensure users create strong passwords are therefore crucial to deploying secure websites. Password strength is a measure of the effectiveness it provides in resisting guessing and brute force attacks. Some of the parameters that help define the password strength include password characteristics such as password length, complexity and randomness.

WebInspect has detected that the current website does not meet the basic guidelines for a secure password.

*The password value used in Login Macro **LoginMacro1** fails to meet these requirements.*

The password does not meet the minimum length requirement of 8 characters.
The password does not contain both uppercase and lowercase alphabets.
The password is not alphanumeric.
The password does not contain special characters.
The password does not contain the required number of tokens. Set of [Letters], [Numbers], [Special characters] are defined as three distinct tokens in WI. To increase the password entropy, it is recommended that the password contain a minimum of 4 of these tokens in any combination.

Note: The assumption is that the username / password used during pen-testing meet the username/password requirement for the web application when deployed live.

Implication

System security is compromised by using weak passwords that can be easily guessed or are an easy target to brute force attacks. Authentication systems fail on compromised passwords as they cannot distinguishbetween impostors and authentic users of the system. Thus, compromising the integrity and confidentiality of the system resources and data.

Fix

The effective strength of the password can be increased by enforcing rules that make the password random and harder to guess.
At a minimum, the password policy should adhere to the following rules:

- The password is at least 8 characters long.
- The password is alphanumeric and contain both letters and numbers.
- The password is a mix of uppercase and lowercase letters.
- The password contains special characters such as #,$ etc
- The password should not contain contextual information such as login credentials, website name etc
- In addition the password strength can be increased by enforcing rules that increase the password randomness. For example, you could require a password have a minimum of 4 tokens, where a token is defined as a set of either [letters], [numbers] or special characters. It is recommended that you implement a password policy that helps increase the password entropy and hence the password strength.

Reference

NIST Computer Security
Estimating Password Strength
NIST Guide to Enterprise Password Management
Special Publication 800-118
OWASP
Authentication Cheat Sheet
Bruce Schneier - Choosing Secure Passwords
Choosing Secure Passwords

Classifications

CWE-521: Weak Password Requirements
http://cwe.mitre.org/data/definitions/521.html

Kingdom: Security Features
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Poor Error Handling: Unhandled Exception (1498)

Summary

Unhandled exceptions are circumstances in which the application has received user input that it did not expect and doesn't know how to deal with. In many cases, an attacker can leverage the conditions that cause these errors in order to gain unauthorized access to the system. Recommendations include designing and adding consistent error-handling mechanisms that are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

Implication

Exception error messages may contain the location of the file in which the offending function is located. This may disclose the webroot's absolute path as well as give the attacker the location of application include files or configuration information. It may even disclose the portion of code that failed. In most cases, it will be the result of the web application attempting to use an invalid client-supplied argument in a SQL statement, which means that SQL injection will be possible. If so, an attacker will at least be able to read the contents of the entire database arbitrarily. Depending on the database server and the SQL statement, deleting, updating and adding records and executing arbitrary commands may also be possible. If a software bug or bug is responsible for triggering the error, the potential impact will vary, depending on the circumstances. The location of the application that caused the error can be useful in facilitating other kinds of attacks. If the file is a hidden or include file, the attacker may be able to gain more information about the mechanics of the web application, possibly even the source code. Application source code is likely to contain usernames, passwords, database connection strings and aids the attacker greatly in discovering new vulnerabilities.

Fix

For Security Operations:

Unknown application testing seeks to uncover new vulnerabilities in both custom and commercial software. Because of this, there are no specific patches or descriptions of this issue. Please note that this vulnerability may be a false positive if the page it is flagged on is technical documentation.However, follow these recommendations to help ensure a secure web application:

- **Use Uniform Error Codes:** Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by using error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Use consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- **Informational Error Messages:** Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft an attack.
- **Proper Error Handling:** Use generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be used by an attacker when orchestrating an attack.

For Development:

This problem arises from the improper validation of characters that are accepted by the application. Any time a parameter is passed into a dynamically-generated web page, you must assume that the data could be incorrectly formatted. The application should contain sufficient logic to handle any situation in which a parameter is not being passed or is being passed incorrectly. Keep in mind how the data is being submitted, as a result of a GET or a POST. Additionally, to develop secure and stable code, treat cookies the same as parameters. The following recommendations will help ensure that you are delivering secure web applications.

- **Stringently define the data type:** Stringently define the data type (a string, an alphanumeric character, etc.) that the application will accept. Validate input for improper characters. Adopt the philosophy of using what is good rather than what is bad. Define the allowed set of characters. For instance, if a field is to receive a number, allow that field to accept only numbers. Define the maximum and minimum data lengths that the application will accept.
- **Verify parameter is being passed:** If a parameter that is expected to be passed to a dynamic Web page is omitted, the application should provide an acceptable error message to the user. Also, never use a parameter until you have verified that it has been passed into the application.
- **Verify correct format:** Never assume that a parameter is of a valid format. This is especially true if the parameter is being passed to a SQL database. Any string that is passed directly to a database without first being checked for proper format can be a major security risk. Also, just because a parameter is normally provided by a combo box or hidden field, do not assume the format is correct. A hacker will first try to alter these parameters while attempting to break into your site.
- **Verify file names being passed in via a parameter:** If a parameter is being used to determine which file to process, never use the file name before it is verified as valid. Specifically, test for the existence of characters that indicate directory traversal, such as .../, c:\, and /.
- **Do not store critical data in hidden parameters:** Many programmers make the mistake of storing critical data in a hidden parameter or cookie. They assume that since the user doesn't see it, it's a good place to store data such as price, order number, etc. Both hidden parameters and cookies can be manipulated and returned to the server, so never assume the client returned what you sent via a hidden parameter or cookie.

For QA:

From a testing perspective, ensure that the error handling scheme is consistent and does not reveal private information about your web application. A seemingly innocuous piece of information can provide an attacker the means to discover additional information that can be used to conduct an attack. Make the following observations:

- Do you receive the same type of error for existing and non-existing files?
- Does the error include phrases (such as "Permission Denied") that could reveal the existence of a file?

Reference

Web Application Security Whitepaper:
http://download.hpsmartupdate.com/asclabs/security_at_the_next_level.pdf

Processing Unhandled Exceptions:
http://www.asp.net/(S(sf10gzjodvrpce55el2p5cnk))/learn/hosting/tutorial-12-cs.aspx

Managing Unhandled Exceptions:
http://www.informit.com/articles/article.aspx?p=32081&seqNum=3

Classifications

CWE-388: Error Handling
http://cwe.mitre.org/data/definitions/388.html

CWE-497: Exposure of System Data to an Unauthorized Control Sphere
http://cwe.mitre.org/data/definitions/497.html

CWE-200: Information Exposure
http://cwe.mitre.org/data/definitions/200.html

Kingdom: Errors
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Cookie Security: Cookie Not Sent Over SSL (4720)

Summary

This policy states that any area of the website or web application that contains sensitive information or access to privileged functionality such as remote site administration requires that all cookies are sent via SSL during an SSL session. The URL: https://uat2-eservice.transglobe.com.tw:443/cs/Logon/Logon.xhtml has failed this policy. If a cookie is marked with the "secure" attribute, it will only be transmitted if the communications channel with the host is a secure one. Currently this means that secure cookies will only be sent to HTTPS (HTTP over SSL) servers. If secure is not specified, a cookie is considered safe to be sent in the clear over unsecured channels.

Fix

For Development:
This issue will ultimately need to be rectified by your Network or Security Operations team. If necessary, implement the change in your development environment.

For Security Operations:

IIS 4.0 and 5.0 Fix Information:
http://support.microsoft.com/default.aspx?scid=kb;en-us;274149

Remediation for IIS 6.x:
http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/0d49cbc8-10e1-4fa8-ba61-c34e524a3ae6.mspx?mfr=true
http://msdn2.microsoft.com/en-us/library/ms998310.aspx

Require SSL for an Authentication Cookie (IIS 7):
http://technet.microsoft.com/en-us/library/cc771633(WS.10).aspx

AnonymousIdentificationSection Class [IIS 7]:
http://msdn.microsoft.com/en-us/library/ms689482.aspx

Use the following links to remediate this issue on an Apache server:
http://search.cpan.org/~jkrasnoo/ApacheCookieEncrypted-0.03/Encrypted.pm
http://hc.apache.org/httpclient-3.x/apidocs/org/apache/commons/httpclient/class-use/Cookie.html

For QA:
This issue will ultimately need to be rectified by your Network or Security Operations team. If necessary, implement the change in your testing environment.

Reference

General Information:
The Unofficial Cookie FAQ

Classifications

CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute
http://cwe.mitre.org/data/definitions/614.html

Kingdom: Security Features
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Cross-Frame Scripting (11294)

Summary

A Cross-Frame Scripting (XFS) vulnerability can allow an attacker to load the vulnerable application inside an HTML iframe tag on a malicious page. The attacker could use this weakness to devise a Clickjacking attack to conduct phishing, frame sniffing, social engineering or Cross-Site Request Forgery attacks.

Clickjacking
The goal of a Clickjacking attack is to deceive the victim user into interacting with UI elements of the attacker’s choice on the target web site without her knowledge and in turn executing privileged functionality on the victim’s behalf. To achieve this goal, the attacker must exploit the XFS vulnerability to load the attack target inside an iframe tag, hide it using Cascading Style Sheets (CSS) and overlay the phishing content on the malicious page. By placing the UI elements on the phishing page to overlap with those on the page targeted in the attack, the attacker can ensure that the victim is forced to interact with the UI elements on the target page not visible to the victim.
WebInspect has detected a response containing one or more forms that accept user input but is missing XFS protection.

An effective frame-busting technique was not observed while loading this page inside a frame.

Execution

Create a test page containing an HTML <iframe> tag whose **src** attribute is set to https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerHeartTip.xhtml. Successful framing of the target page indicates the application’s susceptibility to XFS.
Note that WebInspect will report only one instance of this check across each host within the scope of the scan. The other visible pages on the site may, however, be vulnerable to XFS as well and hence should be protected against it with an appropriate fix.

Implication

A Cross-Frame Scripting weakness could allow an attacker to embed the vulnerable application inside an iframe. Exploitation of this weakness could result in:

Hijacking of user events such as keystrokes
Theft of sensitive information
Execution of privileged functionality through combination with Cross-Site Request Forgery attacks

Fix

Browser vendors have introduced and adopted a policy-based mitigation technique using the X-Frame-Options header. Developers can use this header to instruct the browser about appropriate actions to perform if their site is included inside an iframe. Developers must set the X-Frame-Options header to one of the following permitted values:

- DENY
Deny all attempts to frame the page
- SAMEORIGIN
The page can be framed by another page only if it belongs to the same origin as the page being framed
- ALLOW-FROM origin
Developers can specify a list of trusted origins in the origin attribute. Only pages on origin are permitted to load this page inside an iframe

Developers must **also** use client-side frame busting JavaScript as a protection against XFS. This will enable users of older browsers that do not support the X-Frame-Options header to also be protected from clickjacking attacks.

Reference

HP 2012 Cyber Security Report
The X-Frame-Options header - a failure to launch

Server Configuration:
IIS
Apache, nginx

Specification:
X-Frame-Options IETF Draft

OWASP:
Clickjacking

Frame Busting:
Busting Frame Busting: A Study of Clickjacking Vulnerabilities on Popular Sites
OWASP: Busting Frame Busting

Classifications

CWE-352: Cross-Site Request Forgery (CSRF)
http://cwe.mitre.org/data/definitions/352.html

Kingdom: Security Features
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Privacy Violation: Inconsistent Feedback (11418)

Summary

When entering an invalid username or password during a login, an application may provide meaningful feedback through a response discrepancy. For the potential attacker, this discrepancy increases the chances of a successful brute force attack against the site's authentication.

Execution

Try logging into the application twice, once with an incorrect username and another time with an incorrect password. A generic error message for both attempts indicates a secure application. On the other hand, if there is a difference in the error messages, the application may be providing information that could be used in a brute-force attack.

Implication

Consider an application that takes an email address/username and a password. If the application provides different error messages for a non-existent email address and an incorrect password, it will enable an attacker to submit multiple email addresses and learn about the ones that are actually registered to the application. Being able to enumerate users in an application may enable an attacker to perform a more efficient brute force attack.

Fix

Applications should not indicate specifically whether a user account or password was incorrect, rather a very generic login failure message should be used. For example, during a new user registration or forgotten password function, no meaningful message should be returned to the requestor, rather an email should be sent to the account in question with details of how to reset a forgotten password or reclaim an account.

Reference

OWASP Guide to Authentication
https://www.owasp.org/index.php/Guide_to_Authentication

Username Enumeration Vulnerabilities
http://www.gnucitizen.org/blog/username-enumeration-vulnerabilities

Classifications

CWE-209: Information Exposure Through an Error Message
http://cwe.mitre.org/data/definitions/209.html

Kingdom: Security Features
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Insecure Transport: Weak SSL Protocol (11516)

Summary

HPE Security Fortify WebInspect has detected support for Transport Layer Security Protocol (TLS) 1.1 protocol on the target server. NIST publication 800-52 revision 1 recommends all web applications to prefer Transport Layer Security Protocol version 1.2 (TLS 1.2) and mandates government agencies to develop a migration plan for TLS1.2 by January 2015. TLS1.1 mandates a combination of MD5 and SHA1 for the hash function, which leads to conclusion that strength of TLS1.1 depends largely on the strength of SHA1. MD5 is generally known to be weak. SHA1 use is being phased out. NIST Special Publication 800-131A deprecated the use of SHA-1 in digital signature starting January 2014.

Execution

The list of supported SSL/TLS protocols can be obtained by running the server analyzer tool from HPE security toolkit supplied with HPE Security Fortify WebInspect against the target server.

Implication

Weak TLS/SSL protocols may exhibit any or all of the following properties:

- No protection against man-in-the-middle (MitM) attacks
- Same key used for authentication and encryption
- Weak message authentication control
- No protection against TCP connection closing

These properties can allow an attacker to intercept, modify and tamper with sensitive data.

Fix

Have a migration plan in place for all sites to exclusively use TLS1.2 and above. Disable support for the TLS 1.1 protocol on the server. Instead, TLSv1.2 and above should be used.

- For Apache, modify the following lines in the server configuration

- SSL Protocol ALL –SSLv2 -SSLv3 -TLSv1 –TLSv1.1

- For Nginx, modify the following lines in server configuration:

- SSL_Protocols TLSv1.2

- For IIS, please refer to Microsoft Knowledge Base Articles:

- https://technet.microsoft.com/library/security/3009008

For other servers, please refer to vendor specific documentation.

Reference

NIST Special Publication 800-131A
NIST Special Publication 800-52r1

Classifications

CWE-327: Use of a Broken or Risky Cryptographic Algorithm
http://cwe.mitre.org/data/definitions/327.html

Kingdom: Security Features
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Cookie Security: HTTPOnly not Set (10543)

Summary

The web application does not utilize HTTP only cookies. This is a new security feature introduced by Microsoft in IE 6 SP1 to mitigate the possibility of a successful Cross-Site scripting attack by not allowing cookies with the HTTP only attribute to be accessed via client-side scripts. Recommendations include adopting a development policy that includes the utilization of HTTP only cookies, and performing other actions such as ensuring proper filtration of user-supplied data, utilizing client-side validation of user supplied data, and encoding all user supplied data to prevent inserted scripts being sent to end users in a format that can be executed.

Fix

Reference

References:
https://social.msdn.microsoft.com/Search/en-US?query=HTTPOnly%20Cookie&emptyWatermark=true&ac=5

Classifications

CWE-284: Access Control (Authorization) Issues
http://cwe.mitre.org/data/definitions/284.html

Kingdom: Security Features

http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Web Server Misconfiguration: Server Error Message (10932)

Summary

A server error response was detected. The server could be experiencing errors due to a misbehaving application, a misconfiguration, or a malicious value sent during the auditing process. While error responses in and of themselves are not dangerous, per se, the error responses give attackers insight into how the application handles error conditions. Errors that can be remotely triggered by an attacker can also potentially lead to a denial of service attack or other more severe vulnerability. Recommendations include designing and adding consistent error handling mechanisms which are capable of handling any user input to your web application, providing meaningful detail to end-users, and preventing error messages that might provide information useful to an attacker from being displayed.

Implication

The server has issued a 500 error response. While the body content of the error page may not expose any information about the technical error, the fact that an error occurred is confirmed by the 500 status code. Knowing whether certain inputs trigger a server error can aid or inform an attacker of potential vulnerabilities.

Fix

For Security Operations:

Server error messages, such as "File Protected Against Access", often reveal more information than intended. For instance, an attacker who receives this message can be relatively certain that file exists, which might give him the information he needs to pursue other leads, or to perform an actual exploit. The following recommendations will help to ensure that a potential attacker is not deriving valuable information from any server error message that is presented.

- Uniform Error Codes: Ensure that you are not inadvertently supplying information to an attacker via the use of inconsistent or "conflicting" error messages. For instance, don't reveal unintended information by utilizing error messages such as Access Denied, which will also let an attacker know that the file he seeks actually exists. Have consistent terminology for files and folders that do exist, do not exist, and which have read access denied.
- Informational Error Messages: Ensure that error messages do not reveal too much information. Complete or partial paths, variable and file names, row and column names in tables, and specific database errors should never be revealed to the end user. Remember, an attacker will gather as much information as possible, and then add pieces of seemingly innocuous information together to craft a method of attack.
- Proper Error Handling: Utilize generic error pages and error handling logic to inform end users of potential problems. Do not provide system information or other data that could be utilized by an attacker when orchestrating an attack.

Removing Detailed Error Messages

Find instructions for turning off detailed error messaging in IIS at this link:

http://support.microsoft.com/kb/294807

For Development:

From a development perspective, the best method of preventing problems from arising from server error messages is to adopt secure programming techniques that prevent problems that might arise from an attacker discovering too much information about the architecture and design of your web application. The following recommendations can be used as a basis for that.

- Stringently define the data type (for instance, a string, an alphanumeric character, etc) that the application will accept.
- Use what is good instead of what is bad. Validate input for improper characters.
- Do not display error messages to the end user that provide information (such as table names) that could be utilized in orchestrating an attack.

- Define the allowed set of characters. For instance, if a field is to receive a number, only let that field accept numbers.
- Define the maximum and minimum data lengths for what the application will accept.
- Specify acceptable numeric ranges for input.

For QA:

The best course of action for QA associates to take is to ensure that the error handling scheme is consistent. Do you receive a different type of error for a file that does not exist as opposed to a file that does? Are phrases like "Permission Denied" utilized which could reveal the existence of a file to an attacker? Inconsistent methods of dealing with errors gives an attacker a very powerful way of gathering information about your web application.

Reference

Apache:
Security Tips for Server Configuration
Protecting Confidential Documents at Your Site
Securing Apache - Access Control

Microsoft:
How to set required NTFS permissions and user rights for an IIS 5.0 Web server
Default permissions and user rights for IIS 6.0
Description of Microsoft Internet Information Services (IIS) 5.0 and 6.0 status codes

Classifications

CWE-388: Error Handling
http://cwe.mitre.org/data/definitions/388.html

CWE-497: Exposure of System Data to an Unauthorized Control Sphere
http://cwe.mitre.org/data/definitions/497.html

CWE-200: Information Exposure
http://cwe.mitre.org/data/definitions/200.html

Kingdom: Environment
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Privacy Violation: Autocomplete (11276)

Summary

Most recent browsers have features that will save password field content entered by users and then automatically complete password entry the next time the field are encountered. This feature is enabled by default and could leak password since it is stored on the hard drive of the user. The risk of this issue is greatly increased if users are accessing the application from a shared environment. Recommendations include setting autocomplete to "off" on all your password fields.

Please Note: Recent versions of most browsers, as noted below, now ignore the autocomplete="off" attribute for password fields in html forms. Users are allowed to decide the password policy at their own discretion using the password manager. Although setting is ineffective on these versions of browsers, it would continue to protect website users of earlier versions of these and other browsers that support this attribute.

Browsers NOT Supporting autocomplete="off":

Internet Explorer version 11 or above
Firefox version 30 or above
Chrome version 34 or above
For other browsers, please refer to vendor specific documentation

Execution

To verify if a password filed is vulnerable, first make sure to enable the autocomplete in your browser's settings, and then input the other fileds of the form to see whether the password is automatically filled. If yes, then it's vulnerable, otherwise, not. You may need to do it twice in case it is the first time you type in the credential in your browser.

Please Note: That some modern browsers no longer support this attribute as summarized above. Verification should be done using a browser that supports this attribute.

Implication

When autocomplete is enabled, hackers can directly steal your password from local storage.

Fix

From the web application perspective, the autocomplete can be turned at the form level or individual entry level by defining the attribute AUTOCOMPLETE="off".

Reference

Microsoft:
Autocomplete Security

Classifications

CWE-200: Information Exposure
http://cwe.mitre.org/data/definitions/200.html

Kingdom: Security Features
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Cache Management: Insecure Policy (11306)

Summary

WebInspect has detected a potentially unsafe cache control policy for secure content. While content transmitted over an SSL/TLS channel is expected to guarantee confidentiality, administrators must nonetheless ensure that caching of sensitive content is disabled unless absolutely needed. The misconception that secure content caching is disabled by default by user-agents could cause the application to fail the organization’s cache policy by leaving the secure content cacheable by browsers. Unsafe specification such as Cache-Control: public would instruct the browser to persistently cache the content on the hard drive. Caching can be prevented by specifying one of the following three directives in the response headers

- Cache-control: private
- Cache-Control: no-cache
- Cache-Control: no-store

Execution

Send a request to https://uat2-eservice.transglobe.com.tw:443/cs/Main/OwnerArea/OwnerBankAccountSetting.xhtml and inspect the Cache-Control header value.

Implication

Insecure caching policies could lead to content spoofing or information theft.

SSL provides secure encrypted channel to transfer information from source to user. The information server over SSL is considered sensitive and trusted to be only available to requestor. However, caching these content on disk in temporary internet files or in intermediate proxy server can compromise that trust by exposing it to everyone who has access to these temporary storage or proxy cache. Content served over SSL should have cache disabled.

Fix

Set Cache-Control directive to private, no-cache and/or no-store.

private
This directive allows the server to prevent a shared cache from caching responses that are intended for a single user. The mechanism can be used to ensure that privileged information is not accidentally leaked to unauthorized users. The directive may still allow caching of responses by non-shared caches.

no-cache
For sensitive resources requiring user authentication, servers can send the no-cache directive to prevent caches from serving a cached response without first requiring the user agent to validate the user identity. This directive can be specified with or without field names. When no field names are included, this directive applies to the entire request or response.
When one or more field names are specified in the no-cache directive, the response is can be cached but the specified field(s) must be excluded. If the response must include the specified field, then the cache must ensure that the request triggers a revalidation with the origin server.
Example: Cache-Control: no-cache="Set-Cookie"
This directive can be used to ensure sensitive information leakage by requiring the server to confirm the user identity before serving the protected information.

no-store
To completely disable caching of requests or responses, the server must specify the no-store directive in the Cache-Control header. This directive applies to the entire request and response regardless of whether the directive is sent in the request or the response.

Reference

Server Configuration:
IIS
Apache

HTTP 1.1 Specification:
HTTP Header Field Definitions

OWASP:
Browser Cache FAQ

HTTP Caching:
Tutorial

Classifications

CWE-525: Information Exposure Through Browser Caching
http://cwe.mitre.org/data/definitions/525.html

Kingdom: Environment
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

Insecure Transport: HSTS Not Set (11365)

Summary

Http Strict Transport Security (HSTS) policy enables web applications to enforce web browsers to restrict communication with the server over an encrypted SSL/TLS connection for a set period. Policy is declared via special Strict Transport Security response header. Encrypted connection protects sensitive user and session data from attackers eavesdropping on network connection.
Consider following attack scenarios:

- Users often omit the URI scheme i.e. https:// when typing a URL in location bar to access a website. Also third party websites can link to the site using the “http” scheme instead of "”https”. This could result in an initial connection to a HTTPS-enabled site over an unencrypted channel. An eavesdropping attacker can hijack this unencrypted connection and replace the intended use of HTTPS protocol with HTTP in an attack known as SSLStrip, granting unauthorized access to all subsequent traffic.

- Websites often transfer non-sensitive resources such as help documents over an unencrypted HTTP connection. Any cookies without a secure flag are sent along with such requests potentially disclosing sensitive user and session data to eavesdropper.
- Man-in-the-Middle attacks that exploit user tendencies to override invalid certification warnings, e.g. SSLSniff.

For web sites configured with an accurate HSTS policy, browsers automatically upgrade any HTTP connections to HTTPS. Furthermore, browsers prevent users from overriding any host certificate warnings. HSTS offers an effective defense against above attack scenarios.

Execution

Access location https://uat2-eservice.transglobe.com.tw:443/cs/javax.faces.resource/css/msg.css.xhtml?ln=barcelona-layout and notice the absence of the Strict Transport Security header in the HTTP response.

Implication

A successful MiTM attack such as SSLStrip or SSLsniff can lead to the compromise of sensitive user data such as financial information, Social Security Number, personal information etc. as well as grant unauthorized access to user accounts enabling attackers to perform privileged actions on client's behalf.

Fix

Configure the web application under test to include Strict Transport Security header in every response generated by an HTTPS -enabled site. Any HTTP version of site on the same domain should permanently redirect to the secure encrypted site. Header should not be added to HTTP response as browsers will ignore it.

It is important to note that this header does not prevent from above mentioned attack scenarios during the very first connection to the site or any connections established after the set period has expired. To prevent such a scenario, the site must be added to the pre-loaded HSTS hosts list embedded in both Google Chrome and Mozilla Firefox browsers.

Reference

http://tools.ietf.org/html/rfc6797

Classifications

CWE-319: Cleartext Transmission of Sensitive Information
http://cwe.mitre.org/data/definitions/319.html

Kingdom: Security Features
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html