ASK PENTEST

Malayan Banking Berhad (‘Maybank’)

Web Application Security Assessment for eCustody

September 2017

Confidentiality Notice

The information transmitted in this document is intended only for the addressee and may contain confidential and/or privileges material. Any interception, review, retransmission, dissemination, or the other use of, or taking of any action upon this information by persons or entities other than intended recipients is prohibited by law and may subject them to criminal and/ or civil liability.

DOCUMENT AUTHORIZATION

The enclosed document has been reviewed and accepted by the following people:

Ask Pentest Sdn Bhd

NAME	POSITION	COMPANY	SIGNATURE	DATE

The enclosed document has been verified by the following people:

Malayan Banking Berhad

NAME	POSITION	SIGNATURE	DATE

DOCUMENT AMENDMENT REGISTER

The enclosed document has been amended according to the following description:

#	DATE	REASON	CHAPTER	VERSION	AUTHOR
1.					
2.					
3.					
4.					
5.					

Table of Contents

DEFINITION

Risk level:

Risk Level	Description
Critical	*Severe and may lead to complete loss of confidentiality, controls, services or client/partner confidence. The risk categorized to critical often to be trivial to exploit using publicly available tools or technique.*
High	*Severe or serious loss of confidentiality, controls, services or client/partner confidence.*
Medium	*Significant or medium loss of confidentiality, controls, services or client/partner confidence.*
Low	*Minor loss of confidentiality, controls, services or client/partner confidence.*

CVSS Scoring System:

Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities under the custodianship of the Forum of Incident Response and Security Teams (FIRST). It attempts to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities, so efforts can be prioritized. CVSS scores are based on a series of measurements (called metrics) based on expert assessment ranged from 0 to 10. Vulnerabilities with a base score of 10 are **Critical**, range 7.0-9.9 are **High**, those in the range 4.0-6.9 as **Medium**, and 0-3.9 as **Low**.

CVSS Base Scoring

CVSS Base Scoring attempt to measure qualities intrinsic of vulnerability base on several metric as describe on table below:

Value	Description
Exploitability Metric	
Access Vector (AV) - shows how a vulnerability may be exploited	
Local (L)	*The attacker must either have physical access to the vulnerable system (e.g. firewire attacks) or a local account (e.g. a privilege escalation attack).*
Adjacent Network (A)	*The attacker must have access to the broadcast or collision domain of the vulnerable system (e.g. ARP spoofing, bluetooth attacks).*
Network (N)	*The vulnerable interface is working at layer 3 or above of the OSI Network stack. These types of vulnerabilities are often described as remotely exploitable (e.g. a remote buffer overflow in a network service)*
Access Complexity (AC) - describes how easy or difficult it is to exploit the discovered vulnerability.	
High (H)	*Specialized conditions exist, such as a race condition with a narrow window, or a requirement for social engineering methods that would be readily noticed by knowledgeable people.*

Medium (M)	*There are some additional requirements for access, such as a limit on the origin of the attacks, or a requirement for the vulnerable system to be running with an uncommon, non-default configuration.*
Low (L)	*There are no special conditions for access to the vulnerability, such as when the system is available to large numbers of users, or the vulnerable configuration is ubiquitous.*
Authentication (Au) - describes the number of times that an attacker must authenticate to a target to exploit it	
Multiple (M)	*Exploitation of the vulnerability requires that the attacker authenticate two or more times, even if the same credentials are used each time.*
Single (S)	*The attacker must authenticate once in order to exploit the vulnerability.*
None (N)	*There is no requirement for the attacker to authenticate.*
Impact Metric	
Confidentiality (C) - describes the impact on the confidentiality of processed by the system.	
None (N)	*There is no impact on the confidentiality of the system.*
Partial (P)	*There is considerable disclosure of information, but the scope of the loss is constrained such that not all of the data is available.*
Complete (C)	*There is total information disclosure, providing access to any / all data on the system.*
Integrity (I) - describes the impact on the integrity of the exploited system	
None (N)	*There is no impact on the integrity of the system.*
Partial (P)	*Modification of some data or system files is possible, but the scope of the modification is limited.*
Complete (C)	*There is total loss of integrity; the attacker can modify any files or information on the target system.*
Availability (A) - describes the impact on the availability of the target system.	
None (N)	*There is no impact on the availability of the system.*
Partial (P)	*There is reduced performance or loss of some functionality.*
Complete (C)	*There is total loss of availability of the attacked resource.*

CVSS Temporal Scoring

CVSS Temporal Scoring attempt to measure characteristics that evolve over the lifetime of vulnerability as described in table below:

Value	Description
Exploitability Metric	
Exploitability (E) - the current state of exploitation techniques or automated exploitation code	
Unproven (U)	*No exploit code is available, or the exploit is theoretical.*
Proof-of-concept (P)	*Proof-of-concept exploit code or demonstration attacks are available, but not practical for widespread use. Not functional against all instances of the vulnerability.*
Functional (F)	*Functional exploit code is available, and works in most situations where the vulnerability is present.*
High (H)	*The vulnerability can be exploited by automated code, including mobile code (such as a worm or virus).*

Not Defined (ND)	*This is a signal to ignore this score.*
Remediation level (RL) - current state of mitigation level of the vulnerability	
Official Fix (O)	*A complete vendor solution is available - either a patch or an upgrade.*
Temporary Fix (T)	*There is an official but temporary fix / mitigation available from the vendor.*
Workaround (W)	*There is an unofficial, non-vendor solution or mitigation available - perhaps developed or suggested by users of the affected product or another third party.*
Unavailable (U)	*There is no solution available, or it is ieCustodysible to apply a suggested solution. This is the usual initial state of the remediation level when a vulnerability is identified.*
Not Defined (ND)	*This is a signal to ignore this score.*
Report confidence (RC) - measures the level of confidence in the existence of the vulnerability and also the credibility of the technical details of the vulnerability.	
Unconfirmed (UC)	*A single unconfirmed source, or multiple conflicting sources. Rumored vulnerability.*
Uncorroborated (UR)	*Multiple sources that broadly agree - there may be a level of remaining uncertainty about the vulnerability*
Confirmed (C)	*Acknowledged and confirmed by the vendor or manufacturer of the affected product.*
Not Defined (ND)	*This is a signal to ignore this score.*

Vulnerability References:

Reference	Description
BID	*BugTraq is a full disclosure moderated mailing list for the *detailed* discussion and announcement of computer security vulnerabilities: what they are, how to exploit them, and how to fix them. Each vulnerability is assigned a unique "BugTraq ID" which can be access from URL:* - *http://www.securityfocus.com/bid/<BID>*
CVE	*CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services. Each CVE assigned vulnerability can be access from URL:* - *https://cve.mitre.org/cgi-bin/cvename.cgi?name=<CVE>*
CWE	*CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design. Each CWE assigned weakness can be access from URL:* - *https://cwe.mitre.org/data/definitions/<CWE>.html*

CERT	*The CERT Knowledgebase is a collection of internet security information related to incidents and vulnerabilities. Each security information will be assigned a unique id which can be access from URL:* - *https://www.kb.cert.org/vuls/id/<CERT>*
OSVDB	*Open Sourced Vulnerability Database (OSVDB) is an independent and open-sourced database. The goal of the project is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities. The project promotes greater, open collaboration between companies and individuals. Each vulnerability assigned by OSVDB can be access from URL:* - *http://osvdb.org/show/osvdb/<OSVDB>*

Compliance Result:

Result	Description
Passed	*Configuration value comply with compliance checklist*
Warning	*Configuration not applicable on the system*
Failed	*Configuration value not comply with compliance checklist*

1 EXECUTIVE SUMMARY

1.1 Introduction

Ask Pentest Sdn Bhd ('ASK') performed Web Application Security Assessment for ECUSTODY on behalf of Malayan Banking Berhad ('MAYBANK').

ASK performed the fieldwork from 14 September 2017 to 17 September 2017.

This report contains the details of the exercise including test scope, identified security weaknesses, risks analysis and recommendations to mitigate each weaknesses found during the exercise.

1.2 Background Information

In the past, majority of the security incidents are due to out-dated software, weak configuration and lack of perimeters defense devices such as firewall and IDS. With the maturity of the perimeters defense, most of the attacks are now targeting Application, especially custom web application.

Custom web application share the common risk of attack from typical web application vulnerability such as SQL Injection, Cross Site Scripting, Session manipulation, Remote code injection, etc. Although the attacks are similar, each application could be vulnerable in different way.

Detecting both known attack such as weak configurations, out-dated software / OS to unknown vulnerability that is specific to the application such as SQL Injection, Cross Site Scripting, Session manipulation, etc.

Following guidelines from OWASP Top 10:

i. A1-Injection

ii. A2-Broken Authentication and Session Management

iii. A3-Cross-Site Scripting (XSS)

iv. A4-Insecure Direct Object References

v. A5-Security Misconfiguration

vi. A6-Sensitive Data Exposure

vii. A7-Missing Function Level Access Control

viii. A8-Cross-Site Request Forgery (CSRF)

ix. A9-Using Components with Known Vulnerabilities

x. A10-Unvalidated Redirects and Forwards

1.3 Objective and Scope

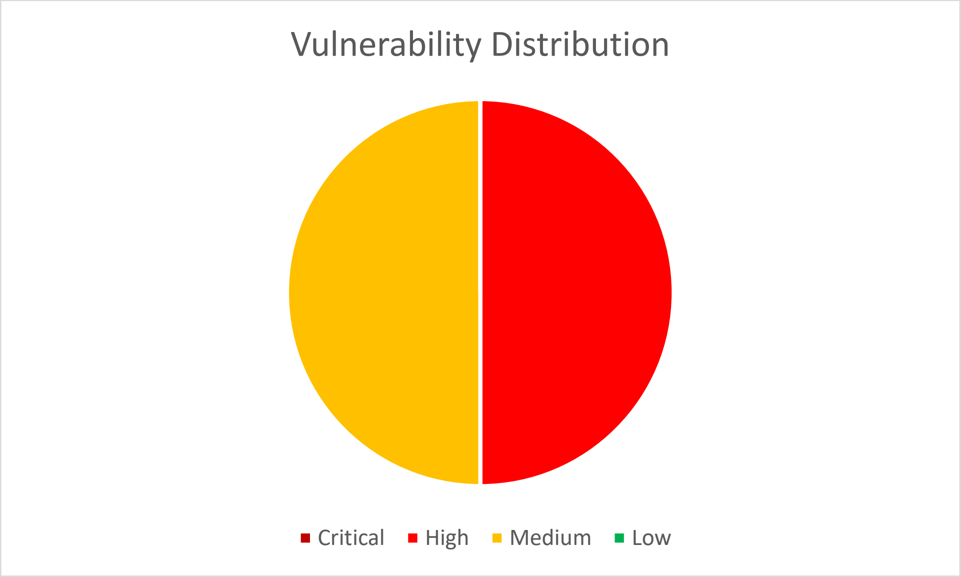
The objective of the exercise was to provide MAYBANK with a point in time assessment of the security controls within the tested system. The assessment result will be a list of known security weaknesses found during the time of the test, together with recommendations for remedial action to increase security level of the tested system.

The security assessment was performed against the following system:

#	Name
1	https://www.maybank2e.net/ecustody/common/Login.do

1.4 Summary of Findings

The figure below demonstrates the distribution of all security weaknesses found base on their risk level and list of technical findings reference which can be found in **SECTION 3** of the report.



	Critical	High	Medium	Low
Findings Reference		3.1.1	3.1.2	
Total	0	1	1	0

1.5 Root Cause Analysis

Several main root causes have been identified which lead to security weaknesses found during the exercise. These root causes can be summarized as follows:

- Cross Site Scripting (XSS)
- Session cookies without HttpOnly flag

2 SUMMARY OF TECHNICAL FINDINGS

2.1 Introduction

This section provides summary information about the security weaknesses identified, including a summary of findings, their business implications, an overview of the testing process, and a matrix containing summary information about weakness found.

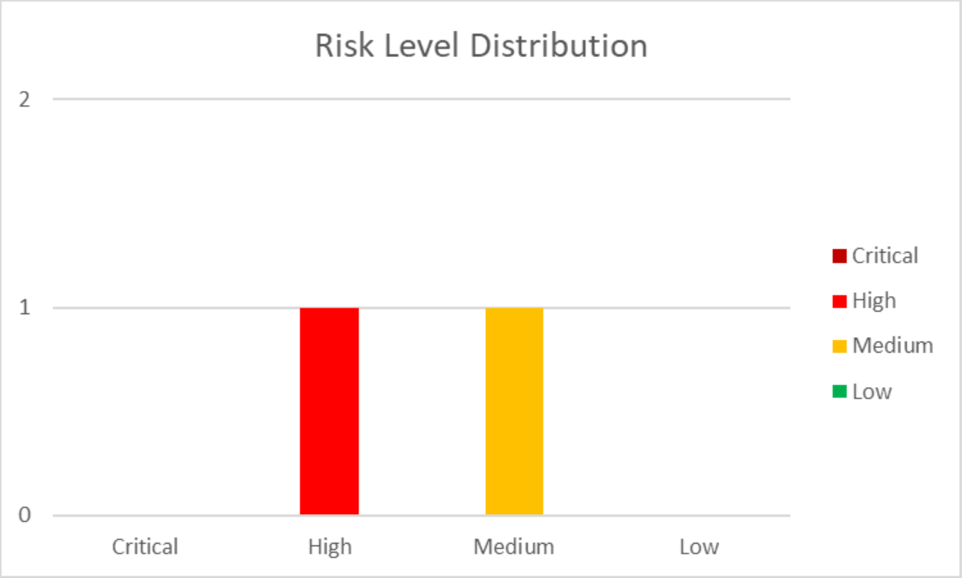
2.2 Risk Level Summary

The table below contains summary of findings found during the exercise:

#	System	Critical	High	Medium	Low	Total
1	https://www.maybank2e.net/ecustody/common/Login.do	0	1	1	0	2
Total		0	1	1	0	2

2.3 Risk Level Distribution

The graph below demonstrate the distribution on findings found during the exercise:



2.4 Findings Matrix

The table below contains a list of all the findings identified during this assessment:

Ref	System	Name	Service	Risk
3.1.1	https://www.maybank2e.net/ecustody/common/Login.do	Cross site Scripting	www (443/tcp)	High
3.1.2	https://www.maybank2e.net/ecustody/common/Login.do	Session cookies without HttpOnly flag	www (443/tcp)	Medium

3 DETAILED TECHNICAL FINDINGS

This section provides details information about the security weaknesses identified during the exercise, including a description of findings, observation process's output, and recommendation to mitigate the issue.

3.1 Findings for https://www.maybank2e.net/ecustody/common/Login.do

3.1.1 Cross Site Scripting (XSS)

Service	Risk	CVSS	CVSS Vector
www (443/tcp)	HIGH	7.1	CVSS2#AV:N/AC:M/Au:N/C:N/I:C/A:N

Vulnerability Status

CVSS Temporal Score	CVSS Temporal Vector	Exploit Available

References

BID	CERT	OSVDB	CWE	CVE
			79	

Description

Cross site scripting (also referred to as XSS) is a vulnerability that allows an attacker to send malicious code (usually in the form of JavaScript) to another user. Because a browser cannot know if the script should be trusted or not, it will execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser.

This vulnerability usually performs in conjunction with phishing attack to make trusted website serve attacker's malicious code such as fake login page or code to steal user's information.

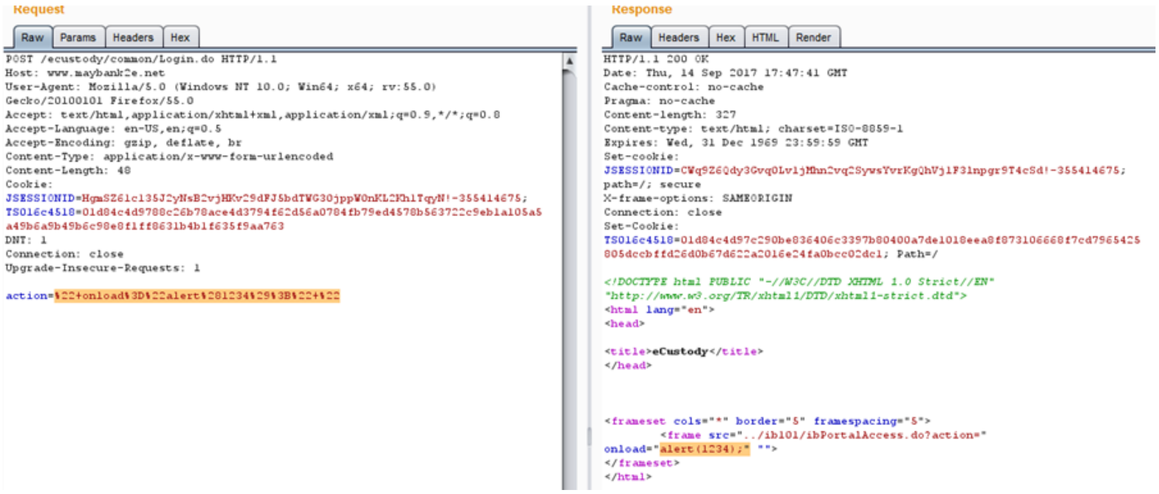
Attacker may inject JavaScript, VBScript, ActiveX, HTML or Flash into a vulnerable application to fool a user to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user and modify the content of the page presented to the user.

There is also possibility for attacker to manipulate HTML code to exploit existing web browser vulnerability such as Windows Metafile vulnerability and infecting the user's system with computer Virus/ Trojan horse.

Affected URL/parameter:

/ecustody/common/Login.do - action

Screen capture



```
POST /ecustody/common/Login.do HTTP/1.1
Host: www.maybank2e.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0)
Gecko/20100101 Firefox/55.0
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 48
Cookie:
JSESSIONID=HgmSZ61c135J2yNsB2vjHKv29dFJ5bdTWG30jppW0nKL2Kh1TqyN!-355414675;
TS016c4518=01d84c4d9788c26b78ace4d3794f62d56a0784fb79ed4578b563722c9eb1a105a5
a49b6a9b49b6c98e8f1ff8631b4b1f635f9aa763
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

action=%22+onload%3D%22alert%281234%29%3B%22+%22
```

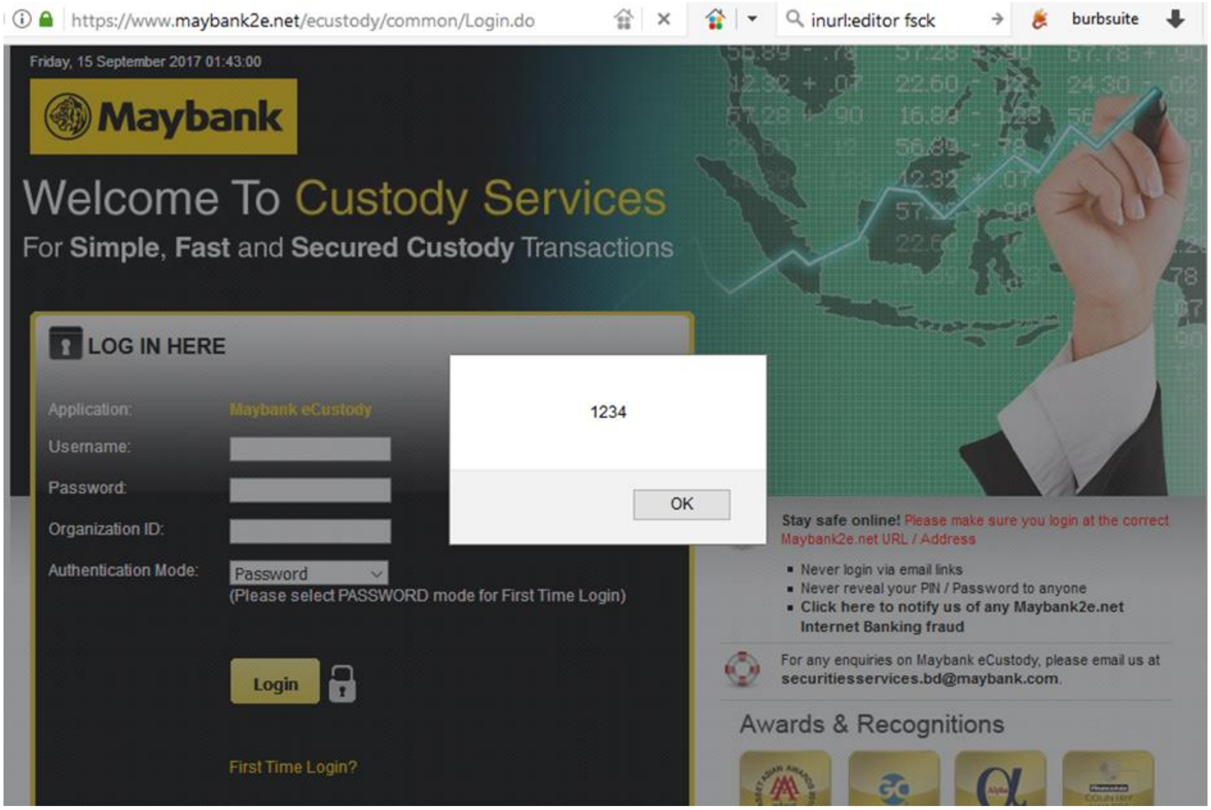
```
HTTP/1.1 200 OK
Date: Thu, 14 Sep 2017 17:47:41 GMT
Cache-control: no-cache
Pragma: no-cache
Content-length: 327
Content-type: text/html; charset=ISO-8859-1
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Set-cookie:
JSESSIONID=CWq9Z6Qdy3GvqOLv1jMhn2vq2SywsYvrKgQhVj1F31npgr9T4cSd!-355414675;
path=/; secure
X-frame-options: SAMEORIGIN
Connection: close
Set-Cookie:
TS016c4518=01d84c4d97c290be836406c3397b80400a7de1018eea8f873106668f7cd7965425
805dccbffd26d0b67d622a2016e24fa0bcc02dc1; Path=/

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html lang="en">
<head>

<title>eCustody</title>
</head>



<frameset cols="*" border="5" framespacing="5">
        <frame src="../ib101/ibPortalAccess.do?action="
onload="alert(1234);" "">
</frameset>
</html>
```



https://www.maybank2e.net/ecustody/common/Login.do

Friday, 15 September 2017 01:43:00

Welcome To Custody Services

For Simple, Fast and Secured Custody Transactions

Application: Maybank eCustody

Username:

Password:

Organization ID:

Authentication Mode: Password
(Please select PASSWORD mode for First Time Login)

First Time Login?

1234

Stay safe online! Please make sure you login at the correct Maybank2e.net URL / Address

- Never login via email links
- Never reveal your PIN / Password to anyone
- Click here to notify us of any Maybank2e.net Internet Banking fraud

For any enquiries on Maybank eCustody, please email us at securitiesservices.bd@maybank.com.

Figure 1.2 : The proof of concept for XSS

Recommendation

Replace HTML special character with HTML special code before display back to user which is:

- < = &lt;
- > = &gt;
- (= &40;
-) = &41
- " = &quot;
- ' = &39;

In some cases where the input being used to generate URL, this character must be convert to URL encoding format.

See also

- http://www.owasp.org/index.php/Cross_Site_Scripting
- http://en.wikipedia.org/wiki/Cross-site_scripting

Management Response

3.1.2 Session cookies without HttpOnly flag

Service	Risk	CVSS	CVSS Vector
www (443/tcp)	Medium	5.0	CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Vulnerability Status

CVSS Temporal Score	CVSS Temporal Vector	Exploit Available

References

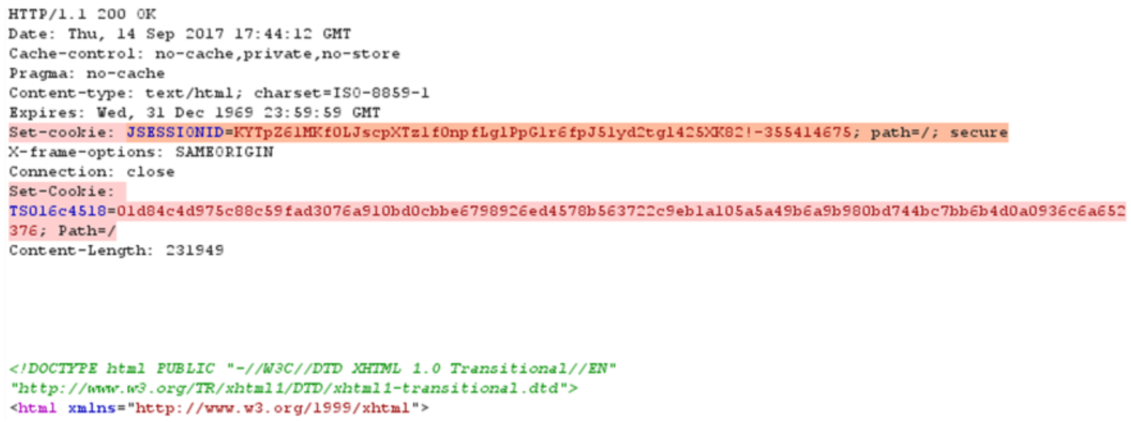
BID	CERT	OSVDB	CWE	CVE
			79	

Description

If the HttpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Affected Cookie: JESSIONID

Screen capture



```
HTTP/1.1 200 OK
Date: Thu, 14 Sep 2017 17:44:12 GMT
Cache-control: no-cache,private,no-store
Pragma: no-cache
Content-type: text/html; charset=ISO-8859-1
Expires: Wed, 31 Dec 1969 23:59:59 GMT
Set-cookie: JSESSIONID=KYTpZ61MKf0LJscpXTz1f0npfLglPpGlr6fpJ5lyd2tgl425XK82!-355414675; path=/; secure
X-frame-options: SAMEORIGIN
Connection: close
Set-Cookie:
TS016c4518=01d84c4d975c88c59fad3076a910bd0cbbe6798926ed4578b563722c9eb1a105a5a49b6a9b980bd744bc7bb6b4d0a0936c6a652
376; Path=/
Content-Length: 231949




<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
```

Figure 1.2 : The proof of concept for session cookie without HttpOnly flag set

Recommendation

Set HttpOnly flag on critical cookies such as session identifier

Management Response