Scan of https://xxxxxxxxxxxxxx/

Scan details

Scan information	
Start time	12/22/2015 3:37:58 PM
Profile	Default

Server information	
Responsive	True
Server banner	Apache-Coyote/1.1
Server technologies	ASP,ASP.NET,PHP,Java/J2EE,FrontPage

Threat level

Threat Level 3

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

Alerts distribution

Total alerts found	**5**	
High	2	🟥
Medium	1	🟧
Low	2	🟦🟦🟦🟦

Open Ports

80/tcp open http Apache httpd 2.4.17 ((Win64) OpenSSL/1.0.2e)

443/tcp open ssl/http Apache httpd 2.4.17 ((Win64) OpenSSL/1.0.2e)

3389/tcp open ssl/ms-wbt-server

Recommendation: port 80 is not offering any service as so it should be closed

Risk High

Vulnerable Javascript library

Vulnerability description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Affected items

/xxxbank/xxxx/js/jquery-ui-1.9.2.custom.js

The impact of this vulnerability

Consult Web References for more information.

How to fix this vulnerability

Upgrade to the latest version.

Web references

http://bugs.jqueryui.com/ticket/6016

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5312

Risk High

Cross Site Scripting

Description

This script is possibly vulnerable to Cross Site Scripting (XSS) attacks.

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.

Impact

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

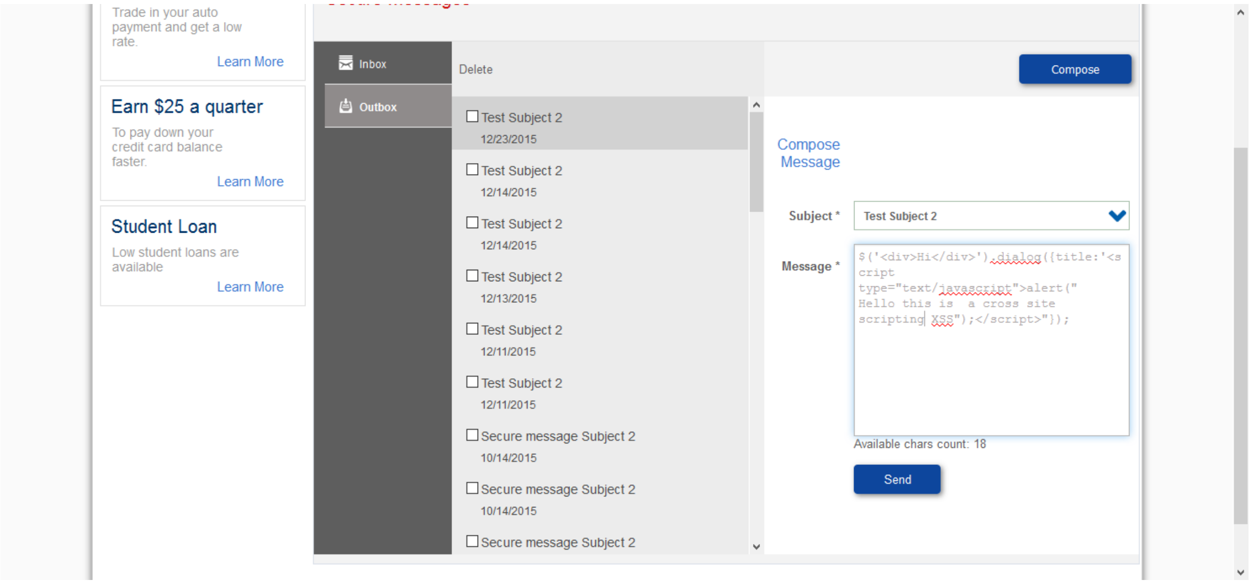
Recommendation

Your script should filter metacharacters from user input and update java library

Affected object

Is the message box at the user and froud reporting send message where it can send the XSS script and

User using the system decides to put an Iframe or link to rederict the staft that reads the messages can do easily.below are the print screens of the XSS



Trade in your auto payment and get a low rate.

Learn More

Earn $25 a quarter

To pay down your credit card balance faster.

Learn More

Student Loan

Low student loans are available

Learn More

□ Test Subject 2
12/23/2015

□ Test Subject 2
12/14/2015

□ Test Subject 2
12/14/2015

□ Test Subject 2
12/13/2015

□ Test Subject 2
12/11/2015

□ Test Subject 2
12/11/2015

□ Secure message Subject 2
10/14/2015

□ Secure message Subject 2
10/14/2015

□ Secure message Subject 2

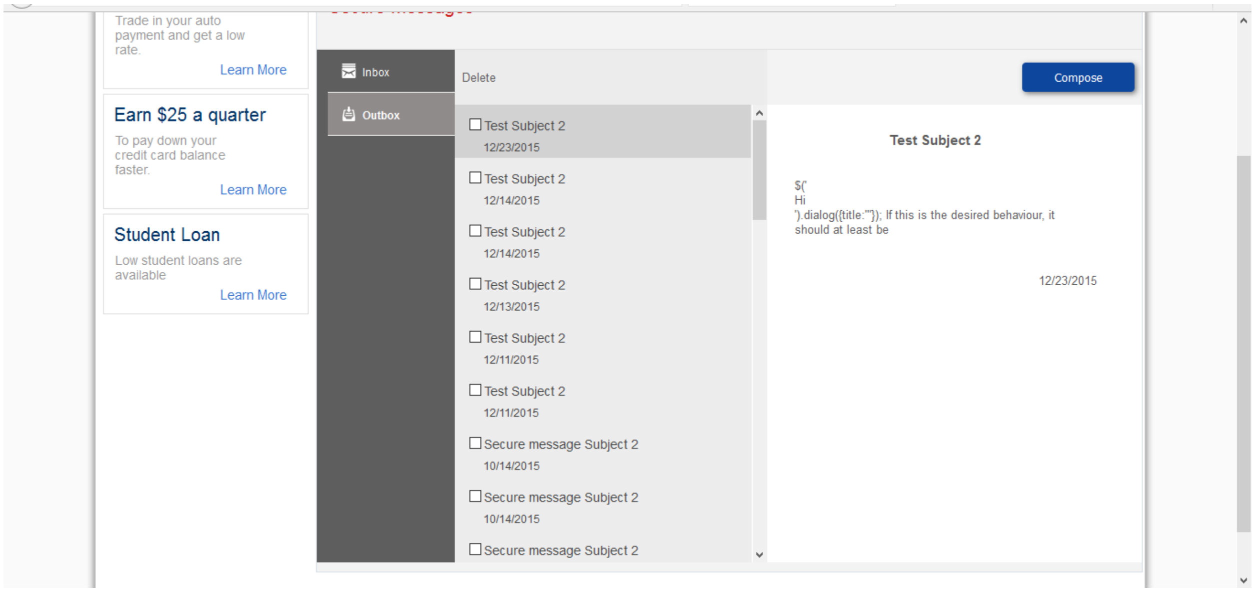
Compose Message

Subject * Test Subject 2

Message *

```
$('<div>Hi</div>').dialog({title:'<s
cript
type="text/javascript">alert("
Hello this is  a cross site
scripting XSS");</script>"});
```

Available chars count: 18



Trade in your auto payment and get a low rate.

Learn More

Earn $25 a quarter

To pay down your credit card balance faster.

Learn More

Student Loan

Low student loans are available

Learn More

□ Test Subject 2
12/23/2015

□ Test Subject 2
12/14/2015

□ Test Subject 2
12/14/2015

□ Test Subject 2
12/13/2015

□ Test Subject 2
12/11/2015

□ Test Subject 2
12/11/2015

□ Secure message Subject 2
10/14/2015

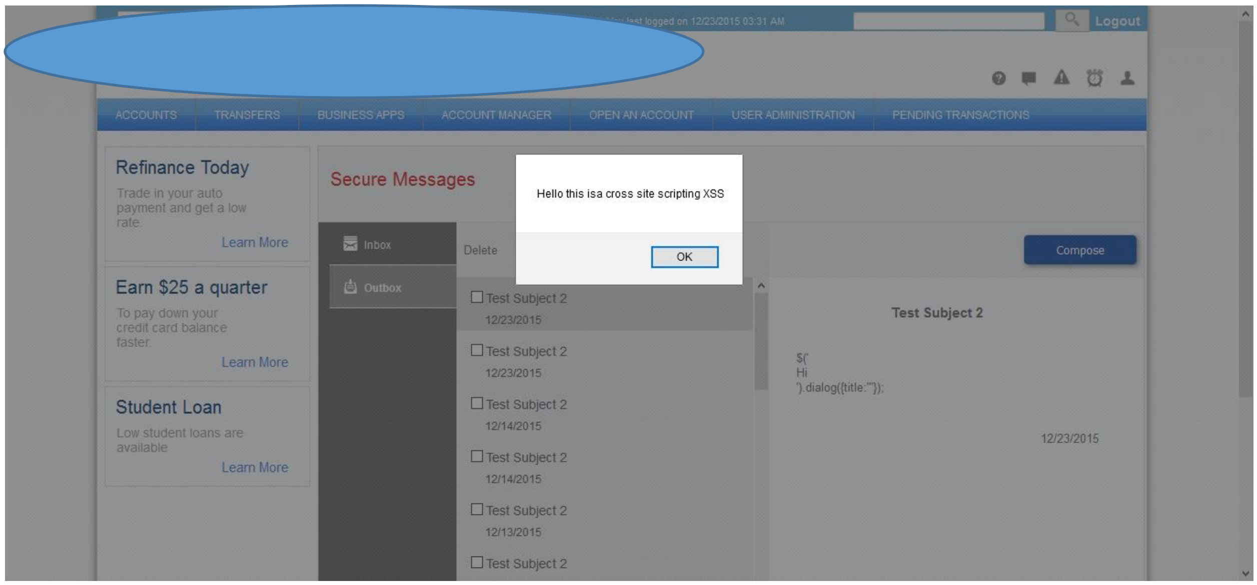
□ Secure message Subject 2
10/14/2015

□ Secure message Subject 2

Test Subject 2

$('
Hi
').dialog({title:''}); If this is the desired behaviour, it
should at least be

12/23/2015



Refinance Today

Trade in your auto payment and get a low rate.

Learn More

Earn $25 a quarter

To pay down your credit card balance faster.

Learn More

Student Loan

Low student loans are available

Learn More

Secure Messages

Hello this isa cross site scripting XSS

□ Test Subject 2
12/23/2015

□ Test Subject 2
12/23/2015

□ Test Subject 2
12/14/2015

□ Test Subject 2
12/14/2015

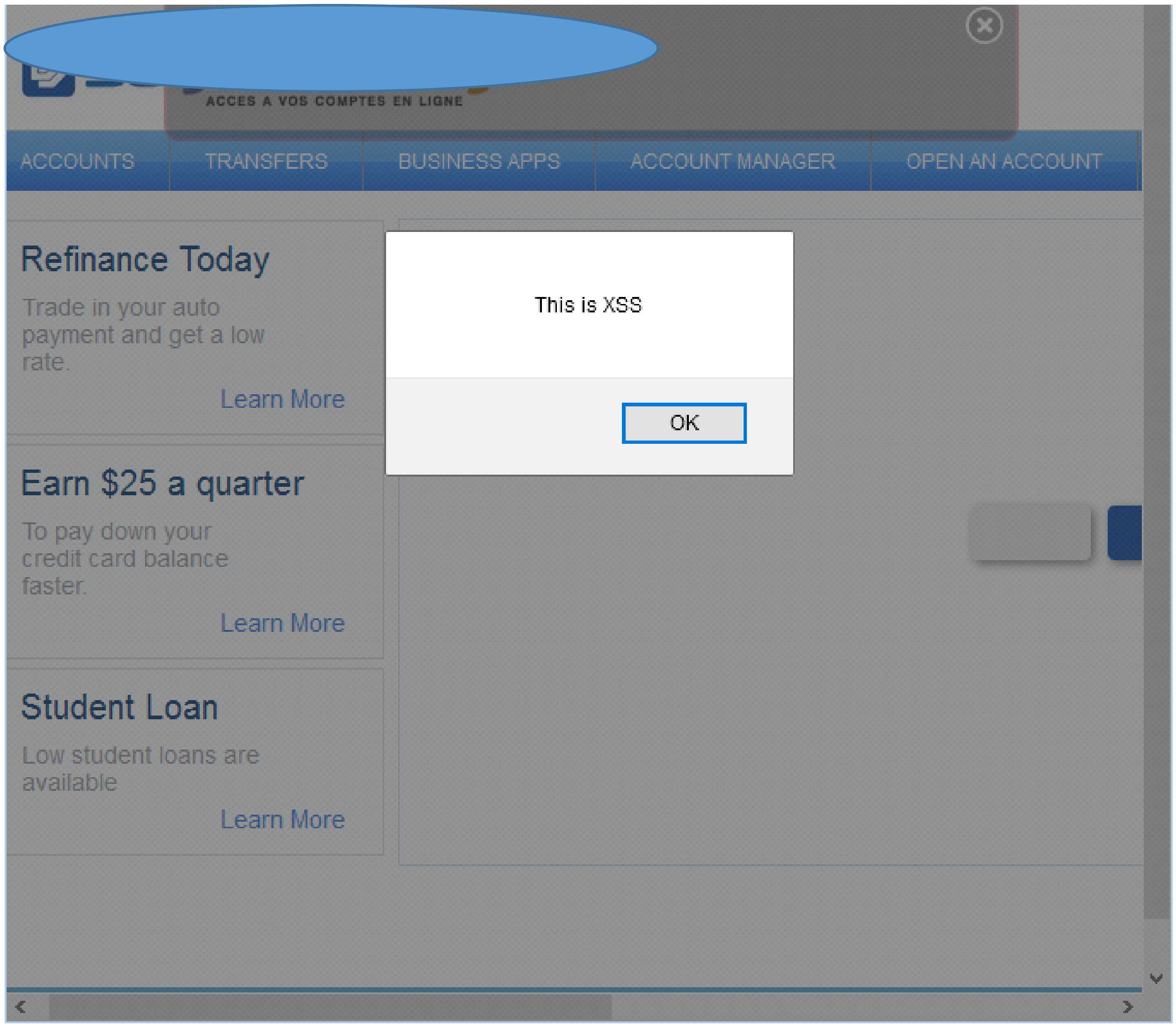
□ Test Subject 2
12/13/2015

□ Test Subject 2

Test Subject 2

```
$('
Hi
').dialog({title:''});
```

12/23/2015


[redacted]

ACCES A VOS COMPTES EN LIGNE

Refinance Today

Trade in your auto payment and get a low rate.

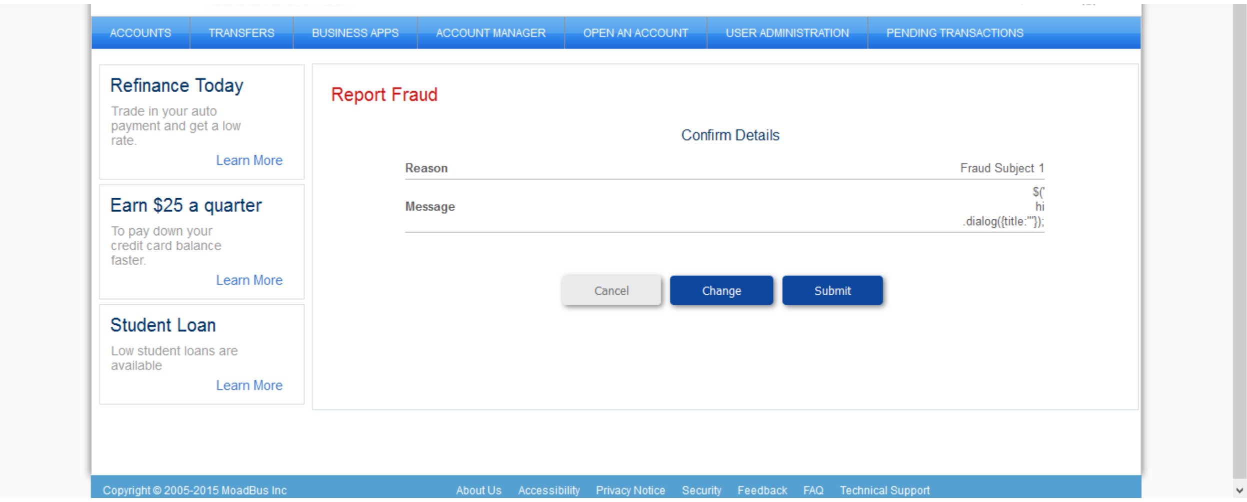
Earn $25 a quarter

To pay down your credit card balance faster.

Student Loan

Low student loans are available

This is XSS



Refinance Today

Trade in your auto payment and get a low rate.

Earn $25 a quarter

To pay down your credit card balance faster.

Student Loan

Low student loans are available

Report Fraud

Confirm Details

Reason	Fraud Subject 1
Message	$(' hi .dialog({title:""});

Copyright © 2005-2015 MoadBus Inc

RISK LOW

Login page password-guessing attack

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

The scanner tested 10 invalid credentials and no account lockout was detected.

Risk Low

Broken links

Description

A broken link refers to any link of the webpage that doesn’t excise this brings generally to an Error page 404 but when is not good configured exposes informations .

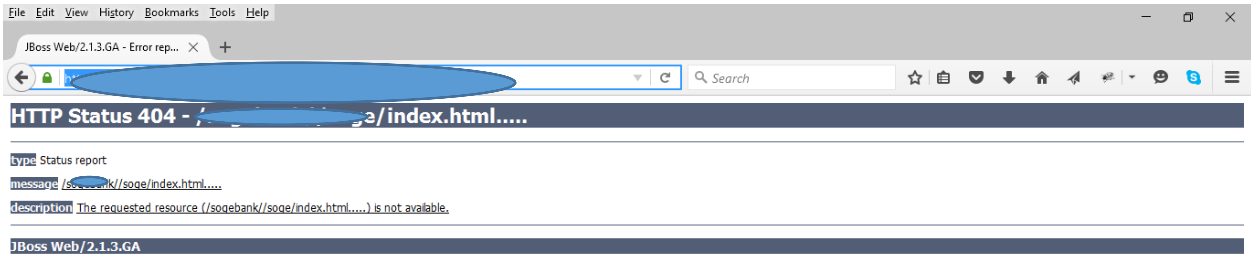
Impact

Information regarding the system , database paths

Recommendation

Error 404 and Error 501 page should be configured properly to show as less information as possible

Affected items
https://cxxxxxxxxxx.....#forward


File Edit View History Bookmarks Tools Help
JBoss Web/2.1.3.GA - Error rep...
Search

[redacted]

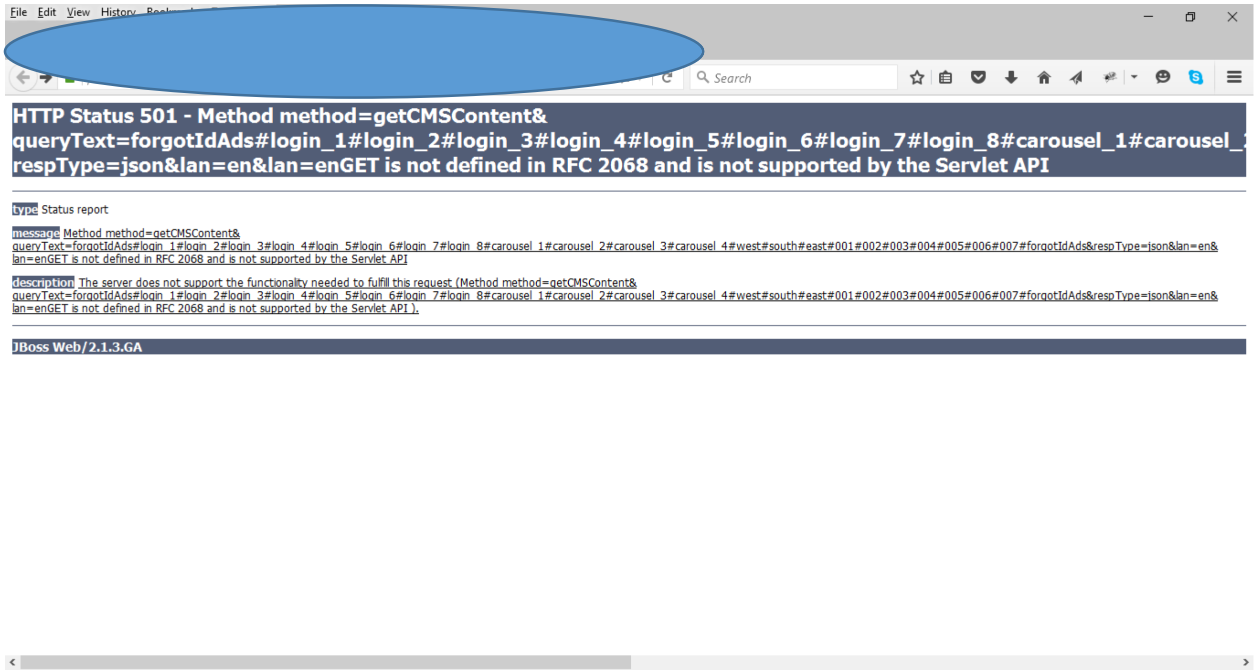
HTTP Status 404 - /[redacted]e/index.html.....

type Status report

message /so[redacted]k//soge/index.html.....

description The requested resource (/sogebank//soge/index.html.....) is not available.

JBoss Web/2.1.3.GA



[redacted]

HTTP Status 501 - Method method=getCMSContent&
queryText=forgotIdAds#login_1#login_2#login_3#login_4#login_5#login_6#login_7#login_8#carousel_1#carousel_
respType=json&lan=en&lan=enGET is not defined in RFC 2068 and is not supported by the Servlet API

type Status report

message Method method=getCMSContent&
queryText=forgotIdAds#login_1#login_2#login_3#login_4#login_5#login_6#login_7#login_8#carousel_1#carousel_2#carousel_3#carousel_4#west#south#east#001#002#003#004#005#006#007#forgotIdAds&respType=json&lan=en&
lan=enGET is not defined in RFC 2068 and is not supported by the Servlet API

description The server does not support the functionality needed to fulfill this request (Method method=getCMSContent&
queryText=forgotIdAds#login_1#login_2#login_3#login_4#login_5#login_6#login_7#login_8#carousel_1#carousel_2#carousel_3#carousel_4#west#south#east#001#002#003#004#005#006#007#forgotIdAds&respType=json&lan=en&
lan=enGET is not defined in RFC 2068 and is not supported by the Servlet API).

JBoss Web/2.1.3.GA

RISK Medium

Slow HTTP Denial of Service Attack

Vulnerability description

Your web server is vulnerable to Slow HTTP DoS (Denial of Service) attacks.

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

Affected items

- Web Server

The impact of this vulnerability

A single machine can take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

How to fix this vulnerability

Consult Web references for information about protecting your web server against this type of attack.

Web references

- Slowloris HTTP DoS
- Slowloris DOS Mitigation Guide
- Protect Apache Against Slowloris Attack

Server Vulnerability testing

Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Description

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

How to fix this vulnerability

- Force the use of SSL as a transport layer for this service if supported, or/and

- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

RDP Screenshot

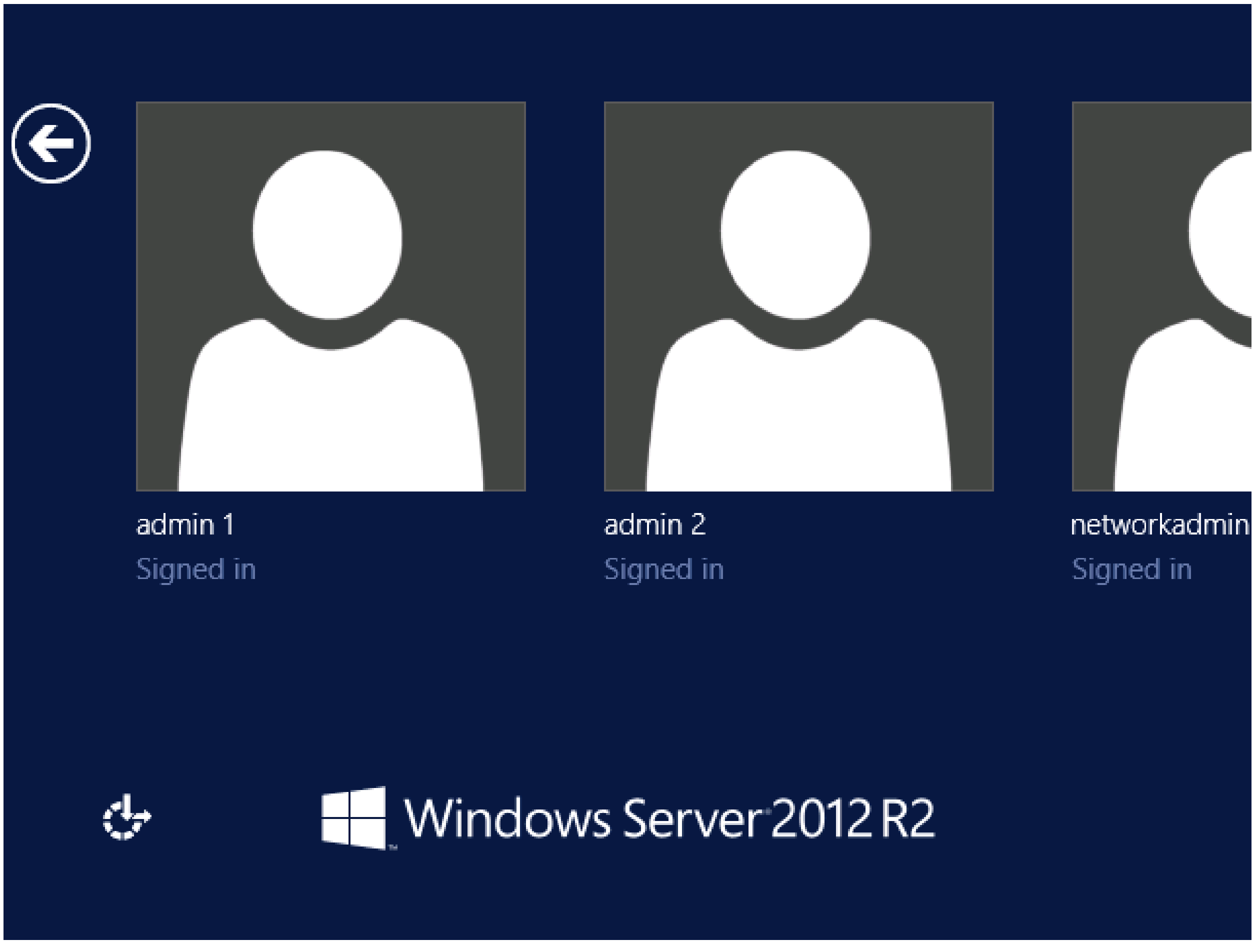
Description

This script attempts to connect to the remote host via RDP (Remote Desktop Protocol) and attempts to take a screenshot of the login screen.

While this is not a vulnerability by itself, some versions of Windows display the names of the users who can connect and which ones are connected already.

Output

- `It was possible to gather the following screenshot of the remote login screen.`


admin 1
Signed in
admin 2
Signed in
networkadmin
Signed in
Windows Server 2012 R2