Web Application Assessment Report

HP WebInspect™

Scan Info

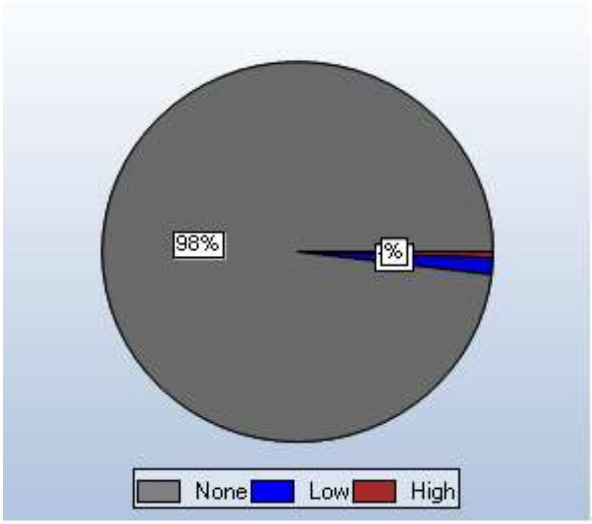
Scan Name	# of Servers	Policy	Date	Duration	Vulns
Site: http://192.168.1.1:8080/	1	Standard	06/01/18	24 mins	5

Server Content

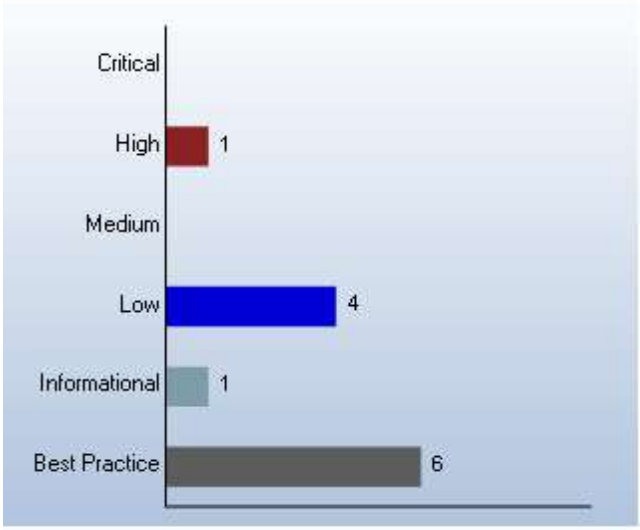
Server	Cookies	Forms	Scripts	External Links	Broken Links	Server Types
http://192.168.1.1:8080	3	5	87	225	21	boa, CGI
Total	3	5	87	225	21	

Vulnerability Summary

Locations With Vulnerabilities



Vulnerability Count



Vulnerability Count by Server

Server	Critical	High	Medium	Low	Info	BP
http://192.168.1.1:8080	0	1	0	4	1	6
Total	0	1	0	4	1	6

Scan Name:	Site: http://192.168.1.1:8080/		
Policy:	Standard	Crawl Sessions:	86
Scan Date:	2018/6/1 14:08:17	Vulnerabilities:	5
Scan Version:	7.0.109	Scan Duration:	24 minutes : 32 seconds
Scan Type:	Site		

Server: http://192.168.1.1:8080

High

跨框架脚本 (11293)

Page: http://192.168.1.1:8080/

Low

可能的文件上功能 (909)

Page: http://192.168.1.1:8080/telecom/manage_device_upgrade.html

服器响 (10932)

Page: http://192.168.1.1:8080/

Page: http://192.168.1.1:8080/<script>alert('TRACE');</script>

Page: http://192.168.1.1:8080/<script>alert('TRACK');</script>

Informational

会令牌 (11287)

Page: http://192.168.1.1:8080/boaform/web_login_exe.cgi

Best Practice

Script File Extension Disclosure (4732)

Page: http://192.168.1.1:8080/boaform/web_login_exe.cgi

Page: http://192.168.1.1:8080/boaform/web_login_exe.cgi?web_login_name=telecomadmin&web_login_password=a7b28c958abd28bbbef4dba863ee3da51d0aacfb849a56c92216a44dccce60dc

Privacy Policy Not Present (5546)

Page: http://192.168.1.1:8080/privacy.html

Page: http://192.168.1.1:8080/privacy.htm

Set-Cookie 不使用 HTTPOnly 关字 （ 10543 ）

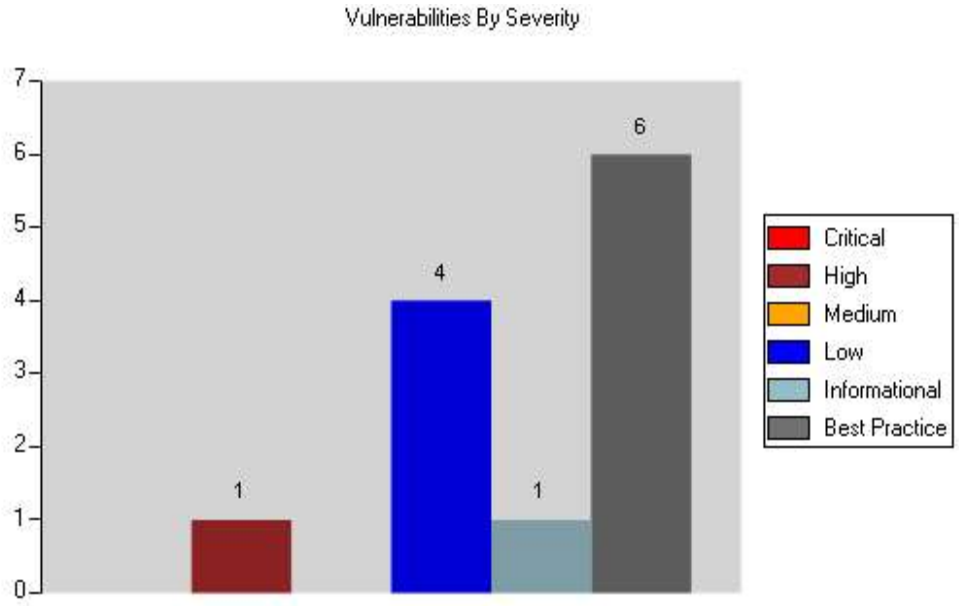
Page: http://192.168.1.1:8080/boaform/web_login_exe.cgi

POST 参数作 GET 参数接受 （ 10655 ）

Page: http://192.168.1.1:8080/boaform/web_login_exe.cgi?
web_login_name=telecomadmin&web_login_password=
a7b28c958abd28bbbef4dba863ee3da51d0aacfb849a56c92216a44dccce60dc

Scan Name:	Site: http://192.168.1.1:8080/		
Policy:	Standard	Crawl Sessions:	86
Scan Date:	2018/6/1 14:08:17	Vulnerabilities:	5
Scan Version:	7.0.109	Scan Duration:	24 minutes : 32 seconds
Scan Type:	Site		

Server: http://192.168.1.1:8080



High 跨框架脚本

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.

Execution:

Create a test page containing an HTML iframe tag whose src attribute is set to http://192.168.1.1:8080/. Successful framing of http://192.168.1.1:8080/ indicates the application's susceptibility to XFS.

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 strictly avoid the use of client-side frame busting JavaScript as a protection against XFS.

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

File Names:
- http://192.168.1.1:8080/

Low 可能的文件上功能

Summary:

找到了文件上功能的。文件上功能允 Web 用将文件从自己的算机送到 Web 服器。如果用于接收文件的 Web 用程序未仔此文件是否包含意内容，那么攻者也能通上文件在服器上行任意命令。建采取格的文件上策略，通清理和避免上意材料。

Implication:

具体影响取决于攻者可以上的文件的性。影响范包括从布未授的内容到助行式攻，直至全面入侵 Web 服器。

Fix:

于安全运部：
此是未知用程序的一部分。未知用程序在自定件和商件中新的漏洞。因此，没有此的特定丁或明。如果面上没有明的文件上功能，大可忽略此。通在示的果上右漏洞点，然后“忽略漏洞”，可以指示描程序忽略此漏洞。

于 QA 部：
需要在生代中解决此。将此通知相的开人。

于开部：

确保行了以下步，以清理将要接收的文件：

- 限制可以上的文件型。例如，在像上面上，拒除 .jpg 以外的任何文件。
- 确保 Web 用没有控制服器上所上文件的名称和位置的限。
- 切勿使用用指定的名称。
- 切勿使用 Web 用的用名和会 ID 派生文件名。
- 不要将文件放在 Web 用可的目中。此位置最好在 Webroot 之外。
- 确保上的文件以及它所在的目置了格的限。
- 不要允在上的文件上行限。如果可能，拒除 Web 用程序用以外的所有用的所有限。
- 确上的文件包含的内容适当。例如，上的 JPEG 具有准的 JPEG 文件。

Classifications:

CWE-434: Unrestricted Upload of File with Dangerous Type
http://cwe.mitre.org/data/definitions/434.html

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

Kingdom: Input Validation and Representation
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/intro.html

File Names:
- http://192.168.1.1:8080/telecom/manage_device_upgrade.html

Low 服器响

Summary:

到服器响。由于行异常的用程序、配置或核程中意的送，可能致服器出。然响本身并没有危，但它可以使攻者了解用程序如何理情况。攻者可程触的可能致拒服攻或其他更重的漏洞。建并添加一致的理机制，它能理 Web 用程序行的任何用入、最用提供有意的信息，同避免示可能攻者提供有用信息的消息。

Implication:

服器已出 500 响。然面的主体内容可能并不会泄漏任何有关技的信息，但事上 500 状代已明生了。了解某些入触服器是否能帮助攻者或向攻者通知存在潜在漏洞。

Fix:

于安全运部：

服器消息（如“文件受限”）常会泄漏多的信息。例如，收到此消息的攻者可以相肯定文件的存在，可能他提供采取其他操作或行攻所需的信息。以下建将有助于确保潜在攻者不会从示的任何服器消息中得到有价的信息。

- 一的代：确保您不会使用不一致或“冲突的”消息而在无意中将信息提供攻者。例如，不要通消息（如“拒”）泄漏非期信息，也会攻者知道他搜索的文件确
- 信息性消息：确保消息不会泄漏多信息。完整或部分路径、量和文件名、表中的行和列
- 适当的理：使用常面和理向最用通知潜在。不要提供可供攻

移除消息

通以下接找关于关 IIS 中消息的明:

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

于开部:

从开角度来，防止由于服器消息生的最佳方法是，采用安全的程方法，使攻者无法有关 Web 用程序体系构和的太多信息。以下建是种做法的基。

- 格定用程序可接受的数据型(例如，字符串、字母数字字符等)。
- 使用肯定的定而非否定的定。入中是否存在不正确的字符。
- 不要向最用示提供的信息(如表名)可用于策划攻的消息。
- 定受允的字符集。例如，如果某个字段要接受数字，使字段接受数字。
- 定用程序接受的最大和最小数据度。
- 指定入可接受的数字范。

于 QA 部:

QA 采取的最佳做法是确保理方案的一致性。相于存在的文件，不存在的文件是否会收到不同型的？是否使用了似于"限被拒"的句，从而可能向攻者泄漏文件是否存在？理的方法不一致就会成攻者收集 Web 用程序相关信息的有效途径。

Reference:

Apache:
有关服器配置的安全提示
保站点上的机密文档
Securing Apache - Access Control

Microsoft:
如何 IIS 5.0 Web 服器置所需的 NTFS 限和用限
IIS 6.0 的默限和用限
Microsoft Internet 信息服 (IIS) 5.0 和 6.0 状代明

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

File Names:
- http://192.168.1.1:8080/
- http://192.168.1.1:8080/<script>alert('TRACE');</script>
- http://192.168.1.1:8080/<script>alert('TRACK');</script>

Informational 会令牌

Summary:

已在此网站以下会令牌:
1. Token=Yqc4kDN62J2P22Q68rwujByBH93o4OL
。

在代 Web 用程序的状方面，会令牌起着关作用。从概念上，会管理系包含存在
客端或服器端的一系列状量，而会令牌(也合称会符或会 ID)用作“密”来
些状量。可以将会令牌置于 cookie、query/post 参数或其他 HTTP 中，它可能由个令牌
成，或在聚合中作多个令牌的集合行引用。
通会令牌，Web 用程序可以跟踪身份的用的活，关用送的求，并向用
提供相的服。当用成功通 Web 用程序的身份，Web 用程序通常会将用的身份与会
令牌关起来，并通引用些令牌来用数据。因此，意攻者可以攻在 Web 用程序中
部署会令牌生的漏洞，从而劫持用会并侵害数据机密性、完整性和可用性。

Execution:

N/A

Implication:

如果意攻者可通易受攻的施会令牌，他可以侵入相的登会并窃取或改敏
感的用数据。特是，如果些会令牌定到管理，整个网站(包括用和其中存的数
据)都有受到侵害的重。

Fix:

N/A

Reference:

Session Management:
http://msdn.microsoft.com/en-us/library/aa478989.aspx

ASP.NET Session State Overview:
http://msdn.microsoft.com/en-us/library/ms178581(v=vs.100).aspx

使用 Java Servlet 技客端状:
http://java.sun.com/j2ee/tutorial/1_3-fcs/doc/Servlets11.html

PHP 会
http://php.net/manual/en/features.sessions.php

OWASP Session Management Cheat Sheet:
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

Classifications:

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

File Names:
- http://192.168.1.1:8080/boaform/web_login_exe.cgi

Best Practice — Script File Extension Disclosure

Summary:

HP 建要求使用已知脚本文件展名的网站或 Web 用程序行，因它可能会致与用程
序所用技相关的信息泄漏。

Execution:

URL http://192.168.1.1:8080/boaform/web_login_exe.cgi 使用已知的脚本展名。

Classifications:

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

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

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

File Names:
- http://192.168.1.1:8080/boaform/web_login_exe.cgi
- http://192.168.1.1:8080/boaform/web_login_exe.cgi?web_login_name=telecomadmin&web_login_password=a7b

Best Practice — Privacy Policy Not Present

Summary:

在您的 Web 用程序上未可用的私策略。与符合性策略有关。多立法倡要求将可公开的文档存放在定了信息私策略的 Web 用程序中。通常，些信息私策略必明将收集哪些信息、收集的目的、潜在的泄漏途径以及解决可能的投的方法。建向 Web 用程序添加可的合私策略，并在求用提供信息的每个面上提供策略的接。

明：

任何准的 Web 用程序私策略都包括下列部分：

- 收集数据的目的描述。
- 关于数据使用情况的描述。
- 限制使用的方法和信息泄漏途径。
- 可能会向其泄漏信息的第三方型列表。
- 用于咨和投的系信息。

Classifications:

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

File Names:
- http://192.168.1.1:8080/privacy.html
- http://192.168.1.1:8080/privacy.htm

Best Practice — Set-Cookie 不使用 HTTPOnly 关字

Summary:

Web 用程序不会利用 HTTP only Cookie。是 Microsoft 在 IE 6 SP1 中引入的新安全功能，禁止通客端脚本具有 HTTP only 属性的 Cookie 行，从而减小跨站点脚本攻成功的可能性。建采用包括利用 HTTP only Cookie 的开策略并采取其他措施，例如确保用提供的数据行正确、用提供的数据行客端，以及用提供的所有数据行以防止将插入的脚本以可行的格式送最用。

Reference:

参考料:
http://msdn.microsoft.com/library/default.asp?url=/workshop/author/dhtml/httponly_cookies.asp

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

File Names:
- http://192.168.1.1:8080/boaform/web_login_exe.cgi

Best Practice POST 参数作 GET 参数接受

Summary:

某些 Web 框架将 POST 和 GET 参数合并成一个集合。从安全角度来，是一种有缺陷的模式。如果面将 POST 参数当作 GET 参数来接受，那么攻者将能通跨站点求造来影响网站的更改，或者利用此缺陷的其他漏洞来攻 Web 用程序所在的系。

Execution:

使用 Web 代理服器工具，到 ~FullUrl~。，将每个 POST 参数添加到 GET 参数列表并重新求面。如果使用 Url 中包含所有 POST 参数的 HTTP GET 求 ~FullUrl~ 行求出相同的面，明此面易受种缺陷的攻。

Implication:

允通 GET 参数 POST 数据参数，可以使 Web 用程序容易受到跨站点求造攻。

Fix:

于开人:
POST 量和 GET 量区分开，不合并两个集合。

于 QA 部:
遵循“行”中列出的明来重此，并开。

于安全运部:
如果使用 Web 框架，告使用 Web 框架的开人将 POST 量与 GET 量区分开，不合并两个集合。

Reference:

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

Classifications:

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

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

File Names:
- http://192.168.1.1:8080/boaform/web_login_exe.cgi?web_login_name=telecomadmin&web_login_password=a7b