



Galactic Defense Force

Vulnerability Assessment Report

for Security Roots, Ltd

Report Version: v0.1
Prepared by: James T. Kirk
Report date: November 20, 2025



Table of Contents

Executive Summary	2
Introduction	2
Scope	2
Conclusions and Recommendations	2
Summary of Findings.....	3
Detailed Internal Findings	6
Blind SQL Injection.....	7
Apache HTTPD: error responses can expose cookies (CVE-2012-0053)	10
Secure HyperText Transfer Protocol (S-HTTP) Detection.....	12
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection.....	13
Detailed External Findings	15
Apache 1.3 HTTP Server Expect Header Cross-Site Scripting	16
Apache Web Server ETag Header Information Disclosure Weakness	18
Host Vulnerability Tables	20
Findings for snorby.org	20
Findings for scanme.insecure.org	20
Findings for 1.1.1.1.....	20
Findings for 10.0.155.160	20
Findings for 173.45.230.150	20
Methodology Tasks Completed	22
Appendices	23
Appendix A: Tools Used	23



Executive Summary

Introduction

The Security Testing team at the Galactic Defense Force is pleased to present the results of the Vulnerability Assessment Report for Security Roots, Ltd.

Scope

The list of hosts covered by this assessment included:

- snorby.org
- scanme.insecure.org
- 1.1.1.1
- 10.0.155.160
- 173.45.230.150

Conclusions and Recommendations

Any data you put in this Description field will export out into the Conclusions and Recommendations section of your welcome pack report template. Use this section to summarize the findings in the report and give high-level recommendations and next steps for your client to take.

Want to add some block code?

https://dradisframework.com/pro/support/guides/word_reports/code_blocks.html

Want to add a screenshot?

https://dradisframework.com/pro/support/guides/word_reports/styles.html#screenshots

Want to add a table?

https://dradisframework.com/pro/support/guides/word_reports/custom_tables.html#create-table



Summary of Findings

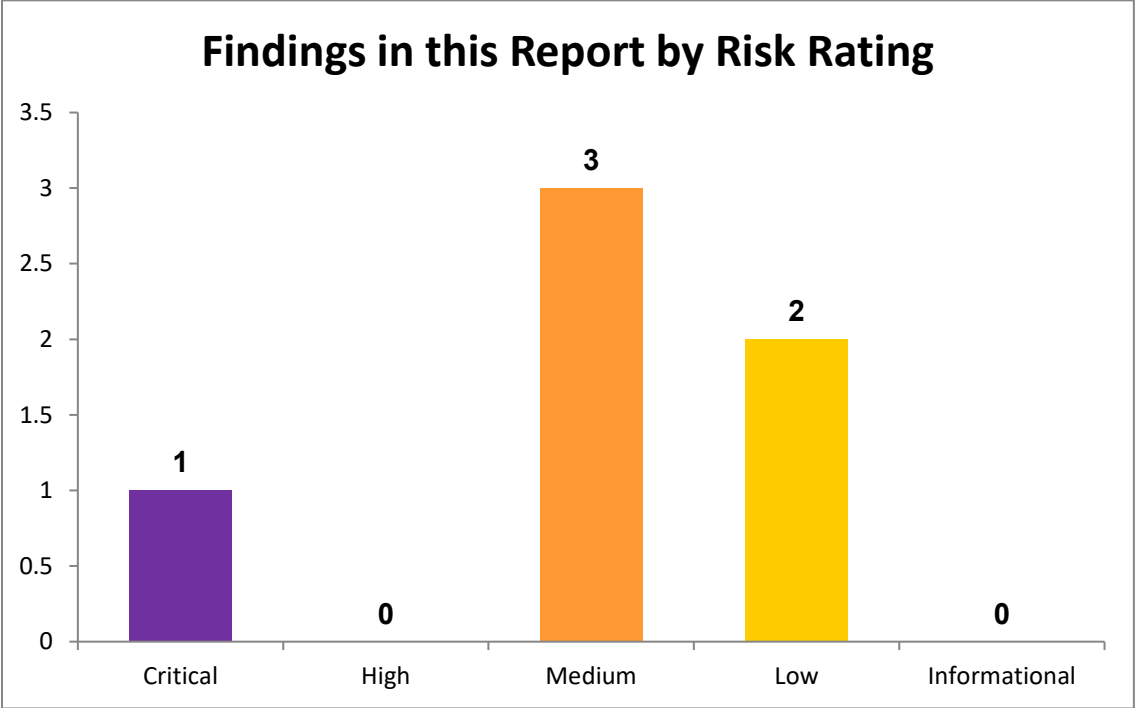
A total of 6 findings were identified. Of these findings, 1 was/were categorized as Critical, 0 was/were categorized as High, 3 was/were categorized as Medium, 2 was/were categorized as Low, and 0 was/were categorized as Informational Risk Rating.

Risk ratings were assigned to findings based on their Common Vulnerability Scoring System (CVSS) base score using the following mapping. To learn more about CVSS, please visit <https://www.first.org/cvss>.

CVSS Score Range	Risk Rating
9.0 to 10.0	Critical
7.0 to 8.9	High
4.0 to 6.9	Medium
0.1 to 3.9	Low
n/a	Informational

A total of 4 findings was/were categorized as Internal, and 2 was/were categorized as External.

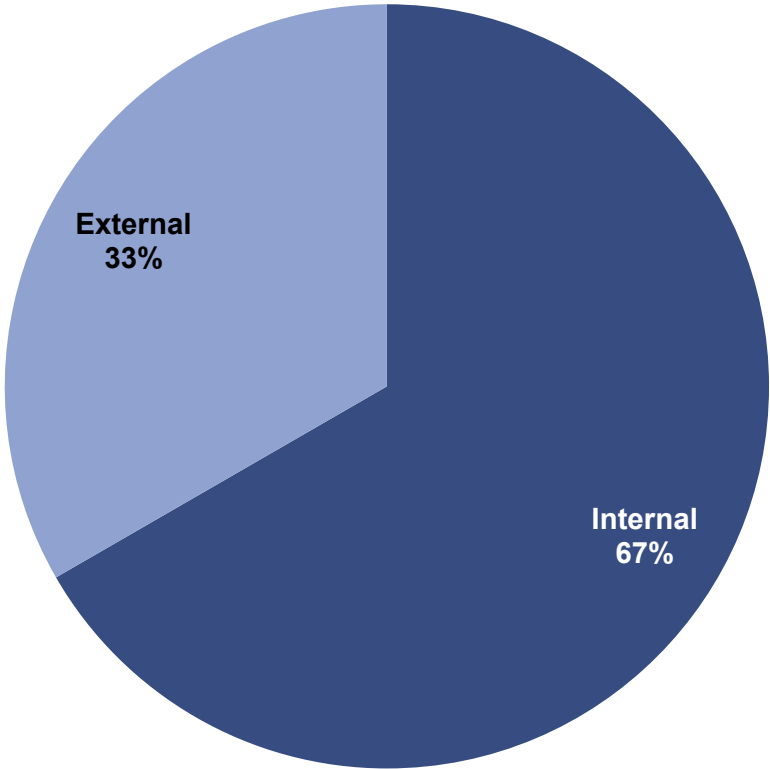
Finding	Risk Rating	Location	Affected Hosts
Blind SQL Injection	Critical	Internal	1.1.1.1
Apache HTTPD: error responses can expose cookies (CVE-2012-0053)	Medium	Internal	1.1.1.1
Apache 1.3 HTTP Server Expect Header Cross-Site Scripting	Medium	External	10.0.155.160
Apache Web Server ETag Header Information Disclosure Weakness	Medium	External	10.0.155.160
Secure HyperText Transfer Protocol (S-HTTP) Detection	Low	Internal	snorby.org, 173.45.230.150
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Low	Internal	snorby.org, 173.45.230.150



CVSS Score Range	Risk Rating	Number of Findings
9.0 to 10.0	Critical	1
7.0 to 8.9	High	0
4.0 to 6.9	Medium	3
0.1 to 3.9	Low	2
n/a	Informational	0



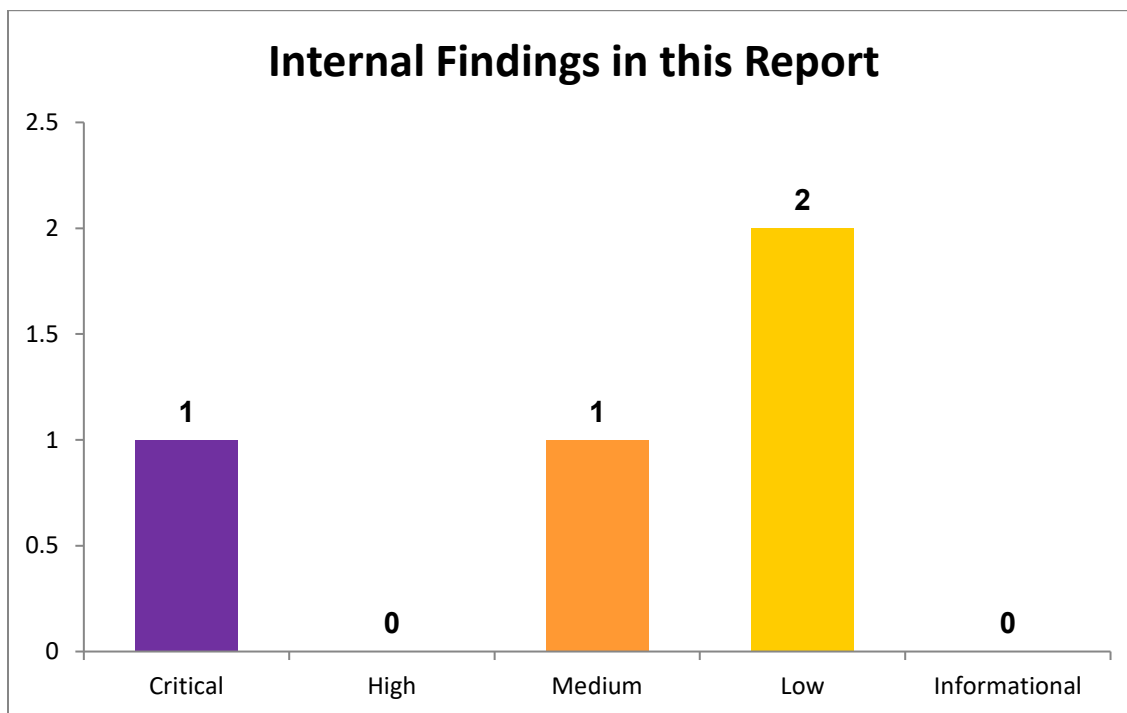
Findings in this Report by Location



Location	Number of Findings
Internal	4
External	2



Detailed Internal Findings



Finding	Risk Rating	Affected Hosts
Blind SQL Injection	Critical	1.1.1.1
Apache HTTPD: error responses can expose cookies (CVE-2012-0053)	Medium	1.1.1.1
Secure HyperText Transfer Protocol (S-HTTP) Detection	Low	snorby.org, 173.45.230.150
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Low	snorby.org, 173.45.230.150



Blind SQL Injection

Rating: Critical

CVSS Score: 9.8

CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Description

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter back-end SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the backend database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use subselects, or append additional queries. In some cases, it may be possible to read in or write out to files or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine type.

Solution

Your script should filter metacharacters from user input.

Check detailed information for more information about fixing this vulnerability.

References

Acunetix SQL Injection Attack

<http://www.acunetix.com/websitesecurity/sql-injection.htm>

<http://www.acunetix.com/blog/web-security-zone/video-sql-injection-tutorial/>

http://www.owasp.org/index.php/Injection_Flaws

<http://www.acunetix.com/websitesecurity/sql-injection2/>

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

http://www.owasp.org/index.php/PHP_Top_5

Evidence for 1.1.1.1

```

      _--_
     /  \_--_
    /    \|__\
   /      \|__\
  /        \|__\
 /          \|__\
/            \|__\
\            /|__\
 \          / |__\
  \        /  |__\
   \      /   |__\
    \    /    |__\
     \  /     |__\
      \/      |__\
       _--_
      /  \_--_
     /    \|__\
    /      \|__\
   /        \|__\
  /          \|__\
 /            \|__\
/              \|__\
\              /|__\
 \            / |__\
  \          /  |__\
   \        /   |__\
    \      /    |__\
     \    /     |__\
      \  /      |__\
       \/_

```

```

~::~~::~~::~~:: http://securityroots.com/dradispro/ ~::~~::~~::~~::
https://10.0.2.15

dradispro login: dradispro
Password:
Last login: Wed Aug 19 01:34:58 EDT 2015 on tty1
Linux dradispro 3.2.0-4-amd64 #1 SMP Debian 3.2.51-1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
dradispro@dradispro:~$ _

```

Page 8 | 23



URL encoded GET input **filter[qty_max]** was set to

(select(0)from(select(sleep(0)))v)/'(select(0)from(select(sleep(0)))v)''(select(0)from(select(sleep(0)))v)''/

Tests performed:

- (select(0)from(select(sleep(3)))v)/'(select(0)from(select(sleep(3)))v)''(select(0)from(select(sleep(3)))v)''/ => **3.266 s**
- (select(0)from(select(sleep(6)))v)/'(select(0)from(select(sleep(6)))v)''(select(0)from(select(sleep(6)))v)''/ => **6.516 s**
- (select(0)from(select(sleep(0)))v)/'(select(0)from(select(sleep(0)))v)''(select(0)from(select(sleep(0)))v)''/ => **1.579 s**
- (select(0)from(select(sleep(9)))v)/'(select(0)from(select(sleep(9)))v)''(select(0)from(select(sleep(9)))v)''/ => **9.344 s**
- (select(0)from(select(sleep(0)))v)/'(select(0)from(select(sleep(0)))v)''(select(0)from(select(sleep(0)))v)''/ => **0.234 s**
- (select(0)from(select(sleep(0)))v)/'(select(0)from(select(sleep(0)))v)''(select(0)from(select(sleep(0)))v)''/ => **0.375 s**
- (select(0)from(select(sleep(0)))v)/'(select(0)from(select(sleep(0)))v)''(select(0)from(select(sleep(0)))v)''/ => **0.454 s**
- (select(0)from(select(sleep(6)))v)/'(select(0)from(select(sleep(6)))v)''(select(0)from(select(sleep(6)))v)''/ => **6.313 s**
- (select(0)from(select(sleep(0)))v)/'(select(0)from(select(sleep(0)))v)''(select(0)from(select(sleep(0)))v)''/ => **0.438 s**

Original value: **1**



Apache HTTPD: error responses can expose cookies (CVE-2012-0053)

Rating: Medium

CVSS Score: 5.2

CVSS Vector: CVSS:3.0/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:L

Description

A flaw was found in the default error response for status code 400. This flaw could be used by an attacker to expose “httpOnly” cookies when no custom ErrorDocument is specified.

Solution

Apache HTTPD ≥ 2.0 and $< 2.0.65$

Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

References

source	text
APPLE	APPLE-SA-2012-09-19-2
BID	51706
CVE	CVE-2012-0053
REDHAT	RHSA-2012:0128
SECUNIA	48551
URL	http://httpd.apache.org/security/vulnerabilities_20.html
URL	http://httpd.apache.org/security/vulnerabilities_22.html

Hosts affected: 1.1.1.1

Evidence for 1.1.1.1

Location: Server



The following NTP variables were found from a readvar request:

```
system="cisco", leap=0, stratum=5, rootdelay=88.21,  
rootdispersion=108.54, peer=24960, refid=135.89.100.96,  
reftime=0xD80BB6B5.715ACDD8, poll=10, clock=0xD80BB78F.8931F3F6,  
phase=8.259, freq=-141.24, error=11.32
```



Secure HyperText Transfer Protocol (S-HTTP) Detection

Rating: Low

CVSS Score: 3.7

CVSS Vector: CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:L

Description

The remote web server accepts connections encrypted using Secure HyperText Transfer Protocol (S-HTTP), a cryptographic layer that was defined in 1999 by RFC 2660 and never widely implemented.

Solution

Rare or obsolete code is often poorly tested. Thus, it would be safer to disable support for S-HTTP and use HTTPS instead.

References

<http://tools.ietf.org/html/rfc2660>

Hosts affected: snorby.org, 173.45.230.150

Evidence for 173.45.230.150

Location: tcp/9090

n/a

Evidence for snorby.org

Location: tcp/9090

n/a



SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection

Rating: Low

CVSS Score: 2.9

CVSS Vector: CVSS:3.0/AV:P/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:L

Description

The remote service encrypts traffic using TLS / SSL but allows a client to renegotiate the connection after the initial handshake. An unauthenticated remote attacker may be able to leverage this issue to inject an arbitrary amount of plaintext into the beginning of the application protocol stream, which could facilitate man-in-the-middle attacks if the service assumes that the sessions before and after renegotiation are from the same 'client' and merges them at the application layer.

Solution

Contact the vendor for specific patch information.

References

<http://extendedsubset.com/?p=8>

<http://www.ietf.org/mail-archive/web/tls/current/msg03948.html>

<http://www.kb.cert.org/vuls/id/120541>

<http://www.g-sec.lu/practicaltls.pdf>

<https://svn.resiprocate.org/rep/ietf-drafts/ekr/draft-rescorla-tls-renegotiate.txt>

Hosts affected: snorby.org, 173.45.230.150

Evidence for 173.45.230.150

Location: tcp/443

n/a

Evidence for snorby.org

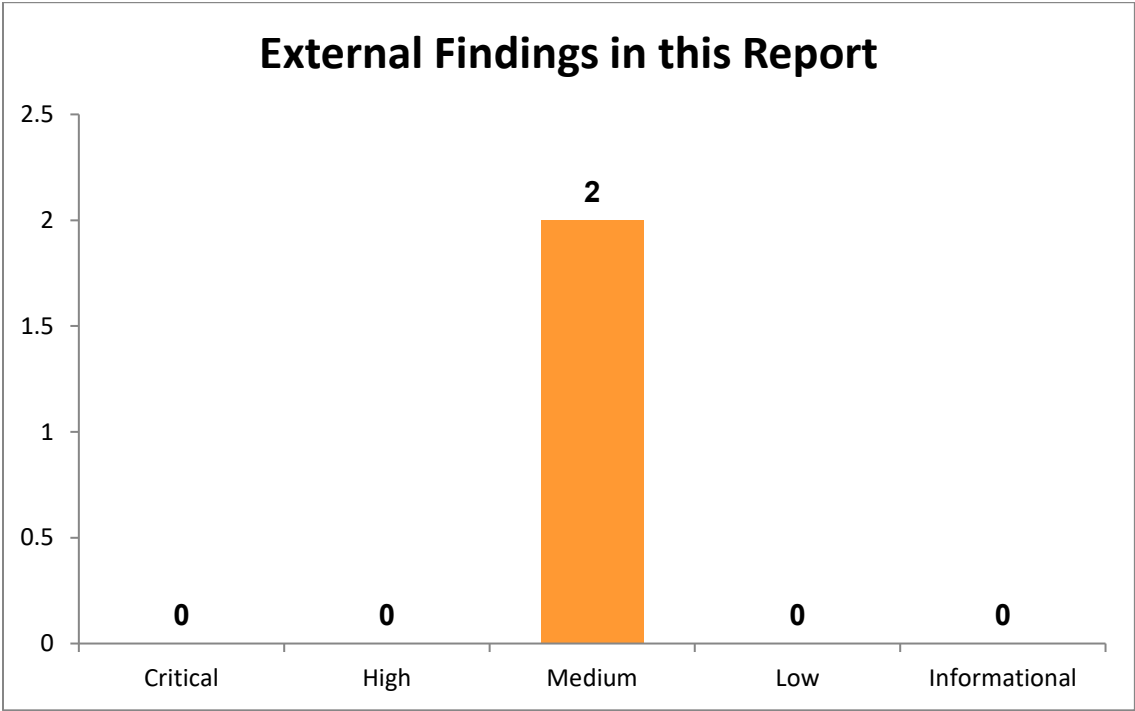
Location: tcp/443

n/a





Detailed External Findings



Finding	Risk Rating	Affected Hosts
Apache 1.3 HTTP Server Expect Header Cross-Site Scripting	Medium	10.0.155.160
Apache Web Server ETag Header Information Disclosure Weakness	Medium	10.0.155.160



Apache 1.3 HTTP Server Expect Header Cross-Site Scripting

Rating: Medium

CVSS Score: 6.4

CVSS Vector:

CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C/CR:M/IR:H/AR:H/MAC:H

Description

A vulnerability exists in Apache HTTP Server Versions 1.3.3 to 1.3.34. This issue occurs due to the handling of invalid Expect headers.

An attacker can exploit this vulnerability to perform a cross-site scripting attack.

Solution

Upgrade to the latest version of Apache, which is available for download from the [Apache Web site](#).

References

Apache 1.3 http://httpd.apache.org/security/vulnerabilities_13.html

Hosts affected: 10.0.155.160

Evidence for 10.0.155.160

Location: tcp/80

```
HTTP/1.1 417 Expectation Failed
Date: Fri, 20 Dec 2011 19:05:57 GMT
Server: Apache
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC " "-//IETF//DTD HTML
2.0//EN">
<HTML><HEAD>
<TITLE>417 Expectation Failed</TITLE>
</HEAD><BODY>
<H1>Expectation Failed</H1>
```



```
The expectation given in the Expect request-header
field could not be met by this server.<P>
The client sent<PRE>
Expect: <script>alert(document.domain)</script>
</PRE>
but we only allow the 100-continue expectation.
</BODY></HTML>
-CR-
```



Apache Web Server ETag Header Information Disclosure Weakness

Rating: Medium

CVSS Score: 4.2

CVSS Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:L

Description

The Apache HTTP Server is a popular, open-source HTTP server for multiple platforms, including Windows, Unix, and Linux.

A cache management feature for Apache makes use of an entity tag (ETag) header. When this option is enabled and a request is made for a document relating to a file, an ETag response header is returned containing various file attributes for caching purposes. ETag information allows subsequent file requests to contain specific information, such as the file's inode number.

A weakness has been found in the generation of ETag headers under certain configurations implementing the FileETag directive. Among the file attributes included in the header is the file inode number that is returned to a client. In Apache Versions 1.3.22 and earlier, it's not possible to disable inodes in ETag headers. In later versions, the default behavior is to release this sensitive information.

This vulnerability poses a security risk, as the disclosure of inode information may aid in launching attacks against other network-based services. For instance, NFS uses inode numbers to generate file handles.

Solution

OpenBSD has released a [patch](#) that fixes this vulnerability. After installing the patch, inode numbers returned from the server are encoded using a private hash to avoid the release of sensitive information.

Customers are advised to upgrade to the latest version of Apache. In Apache Version [1.3.23](#) and later, it's possible to configure the FileETag directive to generate ETag headers without inode information.

To do so, include: "**FileETag -INode**" in the Apache server configuration file for a specific subdirectory.

In order to fix this vulnerability globally, for the Web server, use the option: "**FileETag None**".



Use the option: "`FileETag MTime Size`" if you just want to remove the Inode information.

References

n/a

Hosts affected: 10.0.155.160

Evidence for 10.0.155.160

Location: tcp/80

```
&quot;3bee-4f12-00794aef&quot;;
```



Host Vulnerability Tables

Findings for snorby.org

Finding	Risk Rating	CVSS Score
Secure HyperText Transfer Protocol (S-HTTP) Detection	Low	3.7
SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Low	2.9

Findings for scanme.insecure.org

Finding	Risk Rating	CVSS Score
---------	-------------	------------

Findings for 1.1.1.1

Finding	Risk Rating	CVSS Score
Blind SQL Injection	Critical	9.8
Apache HTTPD: error responses can expose cookies (CVE-2012-0053)	Medium	5.2

Findings for 10.0.155.160

Finding	Risk Rating	CVSS Score
Apache 1.3 HTTP Server Expect Header Cross-Site Scripting	Medium	6.4
Apache Web Server ETag Header Information Disclosure Weakness	Medium	4.2

Findings for 173.45.230.150

Finding	Risk Rating	CVSS Score
Secure HyperText Transfer Protocol (S-HTTP) Detection	Low	3.7



SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Low	2.9
---	-----	-----



Methodology Tasks Completed

OWASPv4 Testing Methodology		
Task Completed	Details	Results
Testing for weak Cryptography	• Testing for Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection (OTG-CRYPST-001) • Testing for Padding Oracle (OTG-CRYPST-002) • Testing for Sensitive information sent via unencrypted channels (OTG-CRYPST-003)	Tester comments
Testing for Error Handling	• Analysis of Error Codes (OTG-ERR-001) • Analysis of Stack Traces (OTG-ERR-002)	Tester comments
Identity Management Testing	• Test Role Definitions (OTG-IDENT-001) • Test User Registration Process (OTG-IDENT-002) • Test Account Provisioning Process (OTG-IDENT-003) • Testing for Account Enumeration and Guessable User Account (OTG-IDENT-004) • Testing for Weak or unenforced username policy (OTG-IDENT-005)	Tester comments



Appendices

Appendix A: Tools Used

Tool	Description
Burp Suite	Burp Suite is an integrated platform for attacking web applications. http://portswigger.net/burp/
Dradis Framework	Collaboration and reporting software for information security teams. https://dradis.com/
Nessus	Nessus is one of the most popular and capable vulnerability scanners, particularly for UNIX systems. http://www.tenable.com/products/nessus-vulnerability-scanner
NeXpose	NeXpose is a vulnerability management software product created by Rapid7. http://www.rapid7.com/products/nexpose/
Nikto	Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items. https://cirt.net/Nikto2
Nmap	Nmap is a free and open source utility for network discovery and security auditing. http://nmap.org/
Metasploit	Metasploit is a penetration testing software created through a collaboration between the open source community and Rapid7. http://www.metasploit.com/
Qualys	Qualys is a cloud-based vulnerability scanner. https://www.qualys.com/
Zed Attack Proxy	The Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project