VNSECURITY

- Home
- Blog
- Papers
- Tools
- About Us
  - VNSECURITY
  - Contact Us
  - CLGT Team
  - How to Join
  - Site Map

- Capture The Flag
- Misc
- Security
  - Anti-Virus
  - Cryptography
  - Exploitation
  - Firewall
  - Forensic
  - Hardening
  - Legal Issues
  - Malware / Rootkit / Hostile Code
  - Mobile Security
  - Physical Security
  - Reverse Engineering
  - Software Security
  - Vulnerabilities
  - Web Security
- Site News
  - VNSECON
- Tiếng Việt

Posts Comments

You are here: Home / Blog / Capture The Flag / CodeGate 2010 Challenge 15 – SHA1 padding attack

CodeGate 2010 Challenge 15 – SHA1 padding attack

March 16, 2010 by RD · 13 Comments

Summary

This is a web based crypto challenge vulnerable to padding/length extension attack in its sha1 based authentication scheme.

Analysis

Challenge URL: http://ctf1.codegate.org/03c1e338b6445c0f127319f5cb69920a/web1.php

This page will ask for submitting a username for the first time. Once a username is submited (‘aaaa’ for example), the script will set a cookie as the following:

```
web1_auth = YWFhYXwx|8f5c14cc7c1cd461f35b190af57927d1c377997e
```

The first part **YWFhYXwx** is the base64 encoded string of *‘aaaa|1'* (username|role). The second part **8f5c14cc7c1cd461f35b190af57927d1c377997e** is the *sha1(unknown_secretkey + username + role)*.

In the next visit, the web1.php script will check for the cookie and return the following message

> “Welcome back, aaaa! You are not the administrator.”

We can guest that 1 is the role value for normal user and 0 for administrator.

Solution

If we try to modify to first part of the web1_auth cookie to something like base64_encode(’aaaa|0'), the script will return an error message saying that the data has been tampered due to the wrong signature.

As we know that popular hash functions including sha1 are vulnerable to length extension (or padding) attacks. This can be used to break naive authentication schemes based on hash functions.

I will not write the detail on how to do sha1 length extension attack, you can read papers in the References section below for more information. Basically, with padding attack, we can append arbitrary data to the cookie and generate a valid signature for it without knowing the secret key. In this challenge, we want to have ‘|0' (administrator role) at the end of the first part of the cookie.

```
$ python sha-padding.py
usage: sha-padding.py <keylen> <original_message> <original_signature>
<text_to_append>

$ python sha-padding.py 25 ‘aaaa|1'
8f5c14cc7c1cd461f35b190af57927d1c377997e ‘|0'
new msg:
‘aaaa|1\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\xf8|0'
base64:
YWFhYXwxgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAD4fDA=
new sig: 70f8bf57aa6d7faaa70ef17e763ef2578cb8d839
```

And here is what we got with the web1_auth cookie using **YWFhYXwxgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAD4fDA=** and signature **70f8bf57aa6d7faaa70ef17e763ef2578cb8d839**

> Welcome back, aaaa! Congratulations! You did it! Here is your flag: CryptoNinjaCertified!!!!!

Source Codes

- http://force.vnsecurity.net/download/rd/shaext.py
- http://force.vnsecurity.net/download/rd/sha-padding.py
- http://force.vnsecurity.net/download/rd/sha.py (this one taken from pypy lib)

References

- http://en.wikipedia.org/wiki/Cryptographic_hash_function
- Flickr's API Signature Forgery Vulnerability
- G. Tsudik, "Message authentication with one-way hash functions," Proceedings of Infocom 92.

Keywords: sha1, padding, length extension attack, codegate 2010

Share and Enjoy:

Filed under Capture The Flag, Cryptography · Tagged with 2010, CLGT, codegate, CTF, length extension attack, padding, sha1

About RD
The man behind the scene

Comments

13 Responses to "CodeGate 2010 Challenge 15 – SHA1 padding attack"

1. *hellman* says:
   March 21, 2010 at 11:29 pm

   how do we now that keylen = 25?

   - *RD* says:
     March 22, 2010 at 9:03 am

     There was a hint from the organizer about the keylen. We can bruteforce the keylen also.

2. *hellman* says:
   March 21, 2010 at 10:56 pm

   no short info about the attack :(

Tweetbacks

Check out what others are saying about this post...

1. *thaidn (Thai Duong)* says:
   March 16th, 2010 at 17:39:34

   Good sha1 length extension exploit – CodeGate 2010 Challenge 15 -http://bit.ly/aKE893 (via @vnsec)

2. *crackinglandia (Nahuel Cayetano Riva)* says:
   March 16th, 2010 at 16:16:14

   RT @vnsec: CodeGate 2010 Challenge 15 – SHA1 padding attack http://bit.ly/aKE893

3. *rcecoder (Gunther)* says:
   March 16th, 2010 at 15:20:51

   RT @vnsec: CodeGate 2010 Challenge 15 – SHA1 padding attack http://bit.ly/aKE893

4. *iamyeh (yeh)* says:
   March 16th, 2010 at 13:29:05

   RT @vnsec: CodeGate 2010 Challenge 15 – SHA1 padding attack http://bit.ly/aKE893

5. *codegate2010 (LM**2)* says:
   March 16th, 2010 at 12:43:59

   RT @phr0nak: @wzzx More about Codegate 2010 write-up's (Challenge 15) http://tinyurl.com/ygdl77a #codegate2010

6. *codegate2010 (LM**2)* says:
   March 16th, 2010 at 12:39:48

RT @vnsec: CodeGate 2010 Challenge 15 – SHA1 padding attack http://bit.ly/aKE893

7. *redragonvn (Thanh Nguyen)* says:
March 16th, 2010 at 12:23:16

   RT @vnsec: CodeGate 2010 Challenge 15 – SHA1 padding attack http://bit.ly/aKE893

8. *vnsec (VNSECURITY)* says:
March 16th, 2010 at 12:14:53

   CodeGate 2010 Challenge 15 – SHA1 padding attack http://bit.ly/aKE893

9. *togakushi (togakushi)* says:
March 16th, 2010 at 12:13:34

   #codegate2010 IRC に貼られたよ。 prob15
   http://www.vnsecurity.net/2010/03/codegate_challenge15_sha1_padding_attack/

10. *phr0nak (phr0nak)* says:
March 16th, 2010 at 12:01:35

   @wzzx More about Codegate 2010 write-up's (Challenge 15) http://tinyurl.com/ygdl77a
   #codegate2010

-
- **VNSEC on Facebook**

  VnSecurity
  Like 379
- You can find most of our members on irc.freenode.net, channel #vnsec.

Follow @vnsec 997 followers

VNSEC Live Tweets

vdchuyen RT @huuloc_n: I'm at Viet My Polyclinic 4sq.com/NAsGbe: đi kéo chm hả mài
3 days ago · reply · retweet · favorite

eugeneteo In Dublin now. Beautiful weather.
4 days ago · reply · retweet · favorite

kaijern Full bar in Rawang #yes4g
6 days ago · reply · retweet · favorite

kaijern only 6 from vt. u.xan.sh/QQuin0 Good old UPX. xandora.net/xangui/malware... #in
13 days ago · reply · retweet · favorite

kaijern From china and access to taiwan DNS server. u.xan.sh/Tk3RU9 #in
13 days ago · reply · retweet · favorite

kaijern I.Love.You.vbs u.xan.sh/O71u86 #xandora #in
13 days ago · reply · retweet · favorite

Join the conversation

- **Archives**

  Select Month

- **Categories**

  Select Category

- **Recent Posts**
  - CodeGate 2012 Quals – Network 400
  - Codegate 2012 Quals – Network 200
  - CodeGate 2012 Quals bin400 writeup
  - CodeGate 2012 Quals bin500 writeup
  - Exploiting Sudo format string vunerability

- **Recent Comments**
  - **Exploiting Sudo format string vunerability (8)**
    - StalkR: sorry, /proc/pid/maps obviously
    - StalkR: nice post longld! @Kenny gdb$ info proc mappings and if you want to see…
  - **Học viện SANS đến Việt Nam 03/2012 (1)**
    - Thiện: Xin vui lòng sửa lại 1 chút, "học viện SANS" thay vì "học việc…
  - **Hack.lu CTF 2011: Nebula Death Stick Services writeup (1)**
    - pants: Is there any chance you could post the actual payload for this? I can start the…

- **Disclaimer**

  VNSECURITY.NET has no relation with any other website called themself VNSECURITY *such as vnsecurity.com (VHF), vnsecurity.vn, vnsecurity.info...*

- **Tags**

  2009 2010 2011 2012 aslr blackhat Capture The Flag CLGT codegate conference Cryptography CTF DDoS debugger DEFCON format string gentoo Hack.lu hackinthebox hitb Israel length extension attack lighttpd mitigate DDoS mitm network NSM OSX padding police renegotiation return-oriented-programming return-to-libc rop ropeme security check sha1 ssl stack guard TEA tls vietnam VNSECON wordpress zine

- **Blogroll**
  - Eugene Teo
  - longld
  - thaidn
  - Xandora
  - Xwings

- **Friends**
  - ARTeam
  - Blue Moon
  - HackInTheBox
  - Sapheads
  - security.org.my
  - The Hacker's Choice
  - Xfocus

Return to top of page

Posts Comments · · Powered by WordPress