CTF TIME

Home / CTF events / Google Capture The Flag 2016 / Tasks / Eucalypt Forest / Writeup

Eucalypt Forest

by atx2600

Tags: crypto

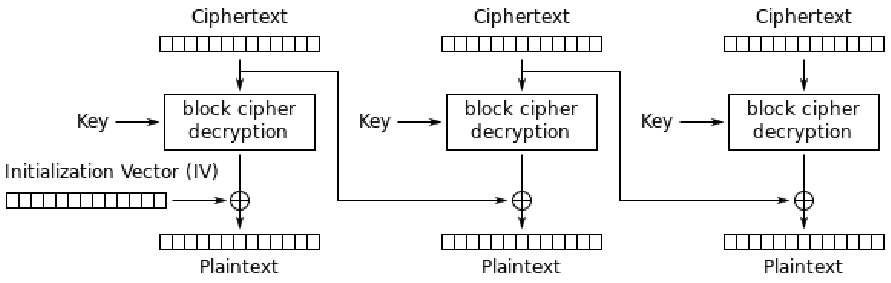
Rating: 0

We are presented with a login system that simply encrypts a JSON blob under AES-CBC, without performing any integrity checks on the data. As such, it is subject to manipulation. Additionally, we have an encryption oracle in the form of a registration script, allowing us to generate a ciphertext of the following form:

{"username":"OUR_USERNAME"}

The only restriction is that OUR_USERNAME cannot be "admin".

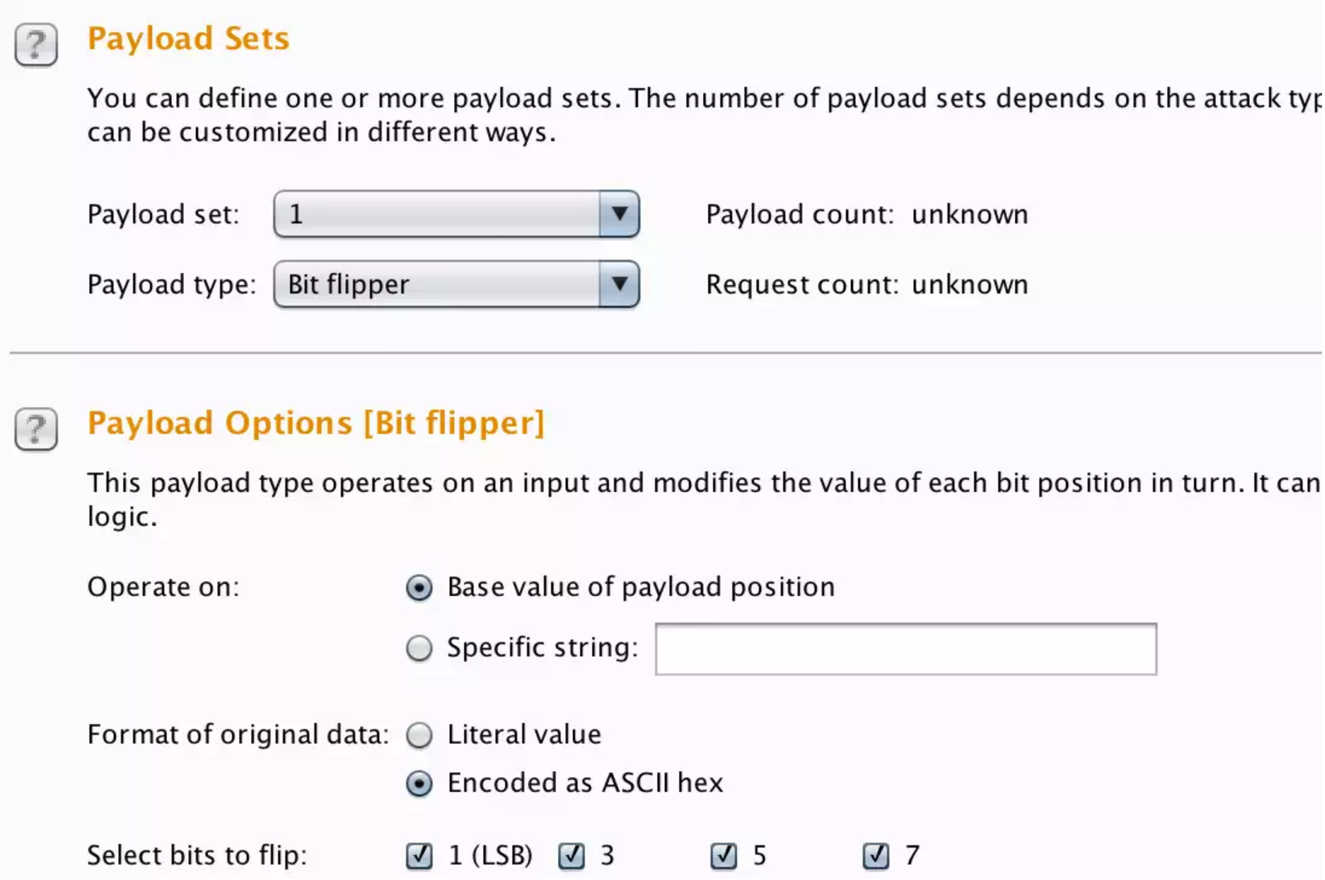
Decryption of AES-CBC ciphertext involves decrypting each block of ciphertext with AES, then performing an XOR operation between the AES-decrypted block and the previous block of ciphertext. For the first block, there is no previous ciphertext block and as such the **Initialization Vector (IV)**, a random block-sized piece of data, is used. Wikipedia has a nice diagram of the process:



Cipher Block Chaining (CBC) mode decryption

When flipping any bit in any block of the ciphertext, it effectively randomizes the decryption of that block. When performing edits to CBC-mode ciphertext, we must either change bits in a block whose meaning is relatively unimportant or, if we have control of the IV, we can modify it to change the first block without any repercussions. Luckily, we do have control of the IV!

We know that the message will take the following form: **{"username":"admin"}**
As such, we can guess that the first two bytes of the username will be at the end of our first block. This means we just need to register a username with one bit off from **admin** and then flip the bits of the resulting authentication cookie until we get access to **/admin**. Flipping the least significant bit of **a (0x61)** gives us **` (0x61)**. We register **`dmin** and then use Burp Intruder to flip the bits like so:



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack typ
can be customized in different ways.

Payload set: 1 ▼ Payload count: unknown

Payload type: Bit flipper ▼ Request count: unknown

Payload Options [Bit flipper]

This payload type operates on an input and modifies the value of each bit position in turn. It can
logic.

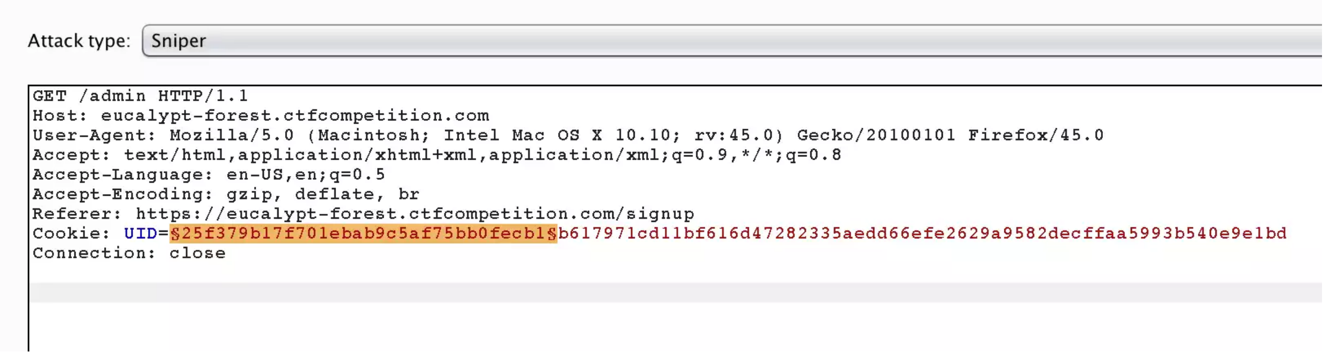
Operate on: ● Base value of payload position

○ Specific string:

Format of original data: ○ Literal value

● Encoded as ASCII hex

Select bits to flip: ☑ 1 (LSB) ☑ 3 ☑ 5 ☑ 7



Attack type: Sniper

```
GET /admin HTTP/1.1
Host: eucalypt-forest.ctfcompetition.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://eucalypt-forest.ctfcompetition.com/signup
Cookie: UID=§25f379b17f701ebab9c5af75bb0fecb1§b617971cd11bf616d47282335aedd66efe2629a9582decffaa5993b540e9e1bd
Connection: close
```

Once we flip the least significant bit of the second to last byte of the IV, we change the username in our ciphertext from "`dmin" to "admin", which gives us access to the admin section, containing the following message:

Note to self - my password is CTF{lettuce.3njoy.our.f00d.puns}

Comments