Internet Security 101

Ulrich Speidel
ulrich@cs.auckland.ac.nz

Scary things out there

- Phishing
- Worms, viruses
- Adware/spyware
- Memes
- Insecure web scripts
- Cross-site scripting
- DDoS attacks
- …and a lot more

Gone phishing…

Worms and viruses

- Viruses rely mostly on user inexperience: infected floppies/CDs/e-mails – require you to install a program or at least insert the disk

- Worms tend to exploit software flaws to propagate: Operating system (interface to the Internet) and e-mail programs are the usual targets. Browsers are also targeted.

Adware/Spyware

- Both adware and spyware offer you some "advantage" – some functionality you find useful
- You "pay" for this by either having to watch ads or surrender information about your (or your user's) surfing behaviour

Spyware example – counter applet

- Counter applet image is offered for "free" inclusion in your web page
- Downloaded from external server to browser
- When downloading, reveals to Spyware server who visits your site, which browser they use, which pages they come from…
- May set cookie on user's browser

Urgent! Your help is needed!

E-MAIL PETITION

The University of Auckland has just announced that lecturers will be required to fail 40% of students in each class. This is part of the university's drive to become New Zealand's leading research university at an international level. A decision to this effect was contained in documents tabled at last week's council meeting.

Lecturers who fail to meet this target risk demotion or bullying by management, says the Association of University Staff (AUS). AUS President Prof. Nigel Haworth says that most of its members disagree completely with this policy. Obviously, this policy is completely unfair and needs to be revoked. It is particularly harsh on international students, single parents, Maori and Pacific Island students and other minority groups.

We, a group of concerned lecturers and professors agree with the union and are looking for student support in this matter. We demand the immediate suspension and retraction of this outrageous policy.

What can you do to help? Add your signature to the bottom of this list and send a copy to everyone you know. Send a cc: to the Vice Chancellor (s.mccutcheon@auckland.ac.nz). We really need as many signatures as possible to prevent disaster. The University must not become an elitist slaughterhouse of your careers! Act now!

Urgent! Your help is needed!

E-MAIL PETITION

The University of Auckland has just announced that lecturers will be required to fail 40% of students in each class. This is part of the university's drive to become New Zealand's leading research university at an international level. A decision to this effect was contained in documents tabled at last week's council meeting.

Lecturers who fail to meet this target risk demotion or bullying by management, says the Association of University Staff (AUS). AUS President Prof. Nigel Haworth says that most of its members disagree completely with this policy. Obviously, this policy is completely unfair and needs to be revoked. It is particularly harsh on international students, single parents, Maori and Pacific Island students and other minority groups.

We, a group of concerned lecturers and professors agree with the union and are looking for student support in this matter. We demand the immediate suspension and retraction of this outrageous policy.

What can you do to help? Add your signature to the bottom of this list and **send a copy to everyone you know**. Send a cc: to the Vice Chancellor (s.mccutcheon@auckland.ac.nz). We really need as many signatures as possible to prevent disaster. The University must not become an elitist slaughterhouse of your careers! Act now!

Yeah right. It's a meme.

Can you trust that bank's web site?

- Sure, it's using strong encryption
- Sure, they have firewalls
- Sure, they have password protection and I have a password that nobody can guess
- Moreover, nobody knows my account number

OK, now what happened here?

- The bank didn't check user input from the login form – a big mistake!
- The hacker passed bits of SQL code in along with the data
- The web script on the bank's server faithfully executed the SQL code passed in
- This particular exploit technique is called *SQL injection*

```
$queryString = "select * from accounttable
                where account= '$account '
                and password= '$password '";
```

OK, now what happened here?

- The bank didn't check user input from the login form – a big mistake!
- The hacker passed bits of SQL code in along with the data
- The web script on the bank's server faithfully executed the SQL code passed in
- This particular exploit technique is called *SQL injection*

```
$queryString = "select * from accounttable
                where account= '123'
                and password= 'sdg!e6273Q '";
```

OK, now what happened here?

- The bank didn't check user input from the login form – a big mistake!
- The hacker passed bits of SQL code in along with the data
- The web script on the bank's server faithfully executed the SQL code passed in
- This particular exploit technique is called *SQL injection*

```
$queryString = "select * from accounttable
                where account='' or password>''
                or password=''
                and password='';
```

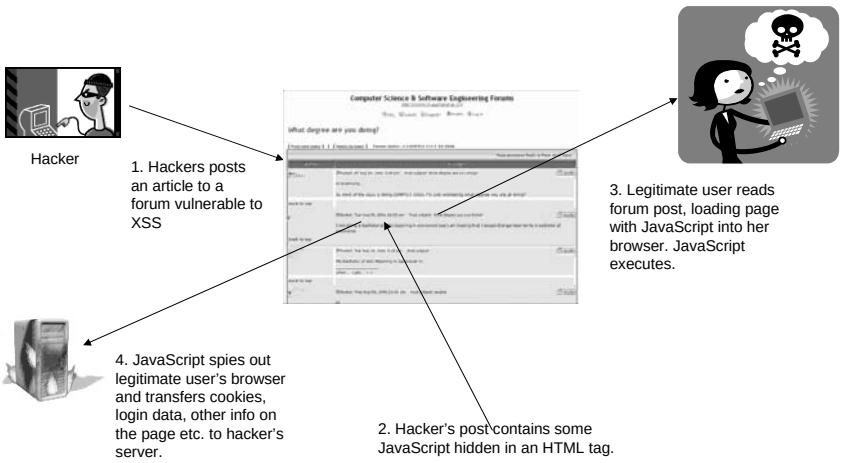
Other types of attacks on web scripts

- Most attacks use crafted input data to make the script do something it wasn't meant to do
- E.g., a file upload can potentially be misused to overwrite a file on the server, plant a web page or even a piece of code such as another script
- Prevention: Filter or escape all input, never use a file name supplied by the browser, carefully look at where user data gets to and can do damage
- Common problem: One of my MSc students found that around 80% of all interactive web scripts in a public archive could be compromised under some circumstances.

Cross-Site-Scripting (XSS)

- Attack on another user of a web site
- Needs a website that doesn't guard against it
- Needs the other user to cooperate
- Preventable by proper escape policy and not allowing HTML markup in posts

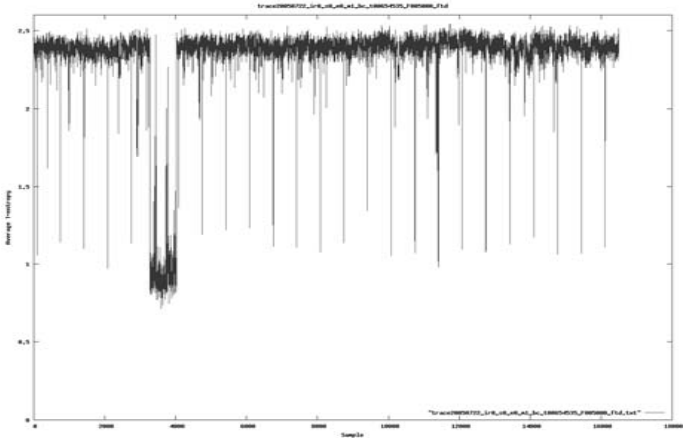
Cross-Site-Scripting (XSS)



(D)DoS

- (Distributed) Denial-of-Service attacks
- Basic idea is simple
- Implementation is also simple
- Very widespread
- Example: Showering a server with bogus connection requests. Server will run out of connection buffers.
- Problem: Detection and mitigation

Detection of (D)DoS & Co.



Work by my PhD research student Raimund Eimann

CS courses that deal with security issues

- COMPSCI334 Internet Programming: scripting security, XSS
- COMPSCI725 Software Security: various topics, focus on copyright and authentication issues as well as the legal and managerial side of security

The End

Thank you for your attention. You may go home now. Take care!