

DEFENSIVE PROGRAMMING

Lecture 10 for EDA 263

Magnus Almgren

Department of Computer Science and
Engineering

Chalmers University of Technology

Traditional Programming

When writing a program, programmers typically focus on what is needed to solve whatever problem the program addresses.

(p.391, Stallings/Brown)

- Common assumptions:
 - inputs a program will receive,
 - environment the program runs in,
 - a “cooperative” user, etc.

Defensive Programming

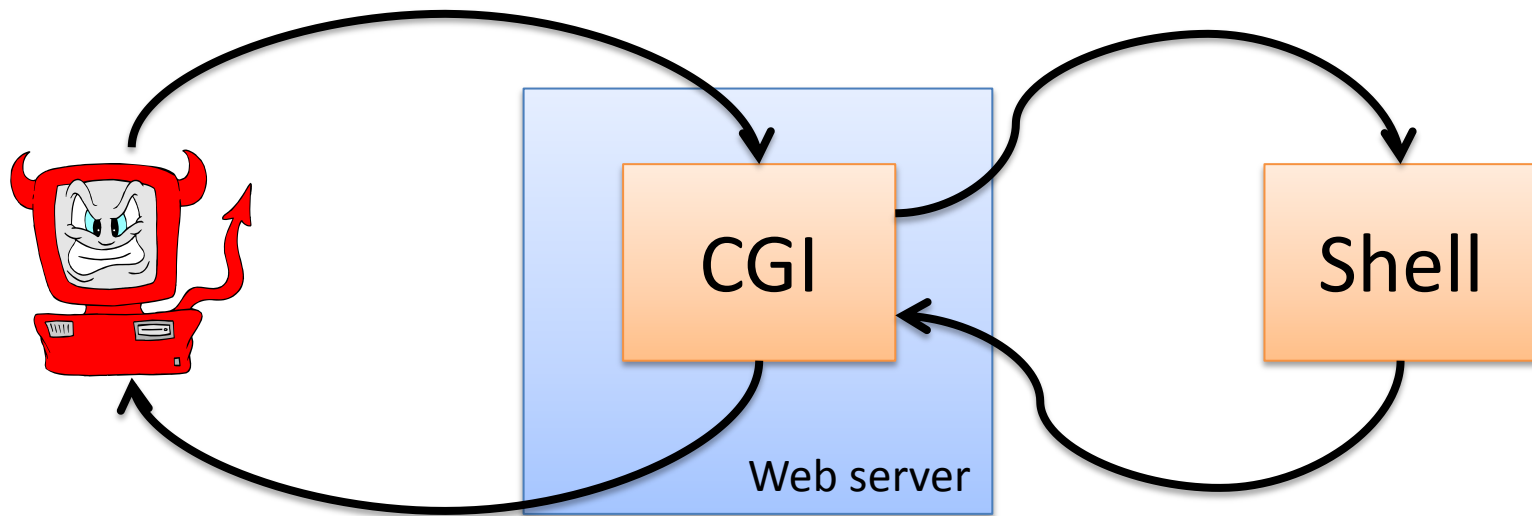
One should always take care when writing a program – code is reused and it is impossible to foresee how and when a module will be used in the future. ***Never trust user input!***

- Defensive programming / Secure Programming:
 - must always validate assumptions (nothing is assumed),
 - needs an awareness of the consequences of failures, and
 - the techniques used by attackers.
- Range of similar vulnerabilities exploited over time (CERT)
 - Injection Attacks (ex 12.2)
- Examples
 - Databases: part of almost all real systems
 - Web apps: often done quickly by junior programmers, but accessible by anyone in the world (see OWASP list)

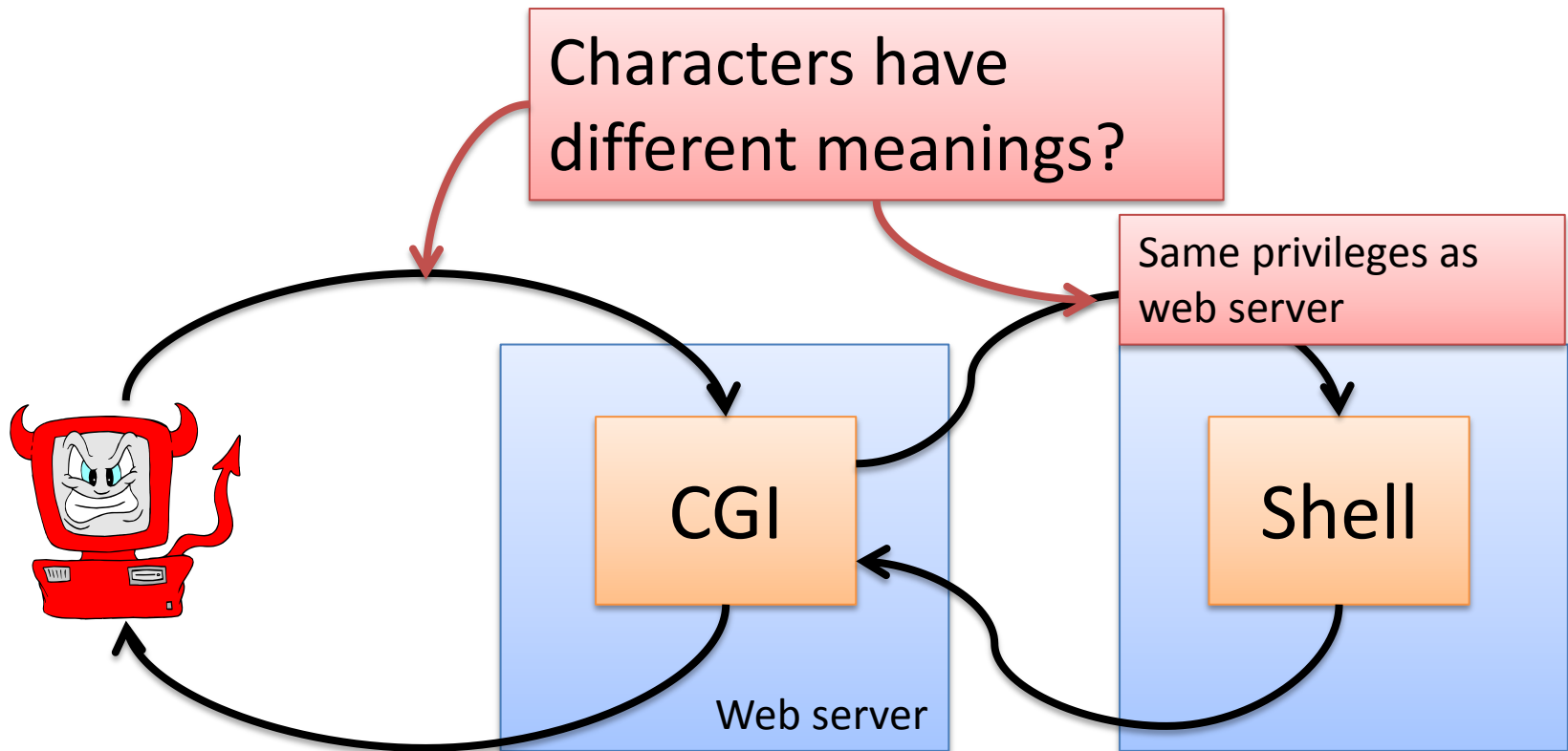
Domains

- Handling Program Input
 - Buffer Overflows
 - Injections Attacks
- Writing Safe Program Code
- Interacting with OS and other programs
- Handling Program Output

Example: Command Injection



Example: Command Injection



Example: Command Injection Mitigation Technique

- Define what is known dangerous input
- Define what is valid input
- Problems:
 - Definition of what is really dangerous
 - Multiple encodings
 - For web: space = %20, / = %2F, ; = %3B
- Not only for strings but also other types of data: *integer overflows*



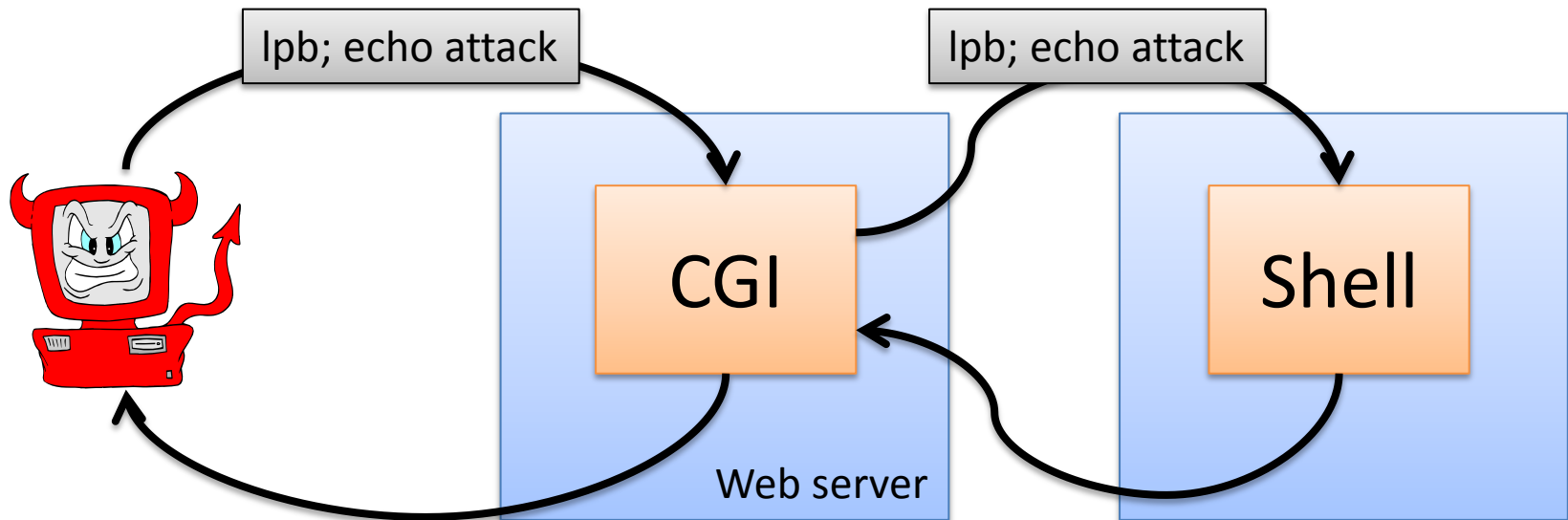
<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=01219077>

Vulnerability Note VU#20276

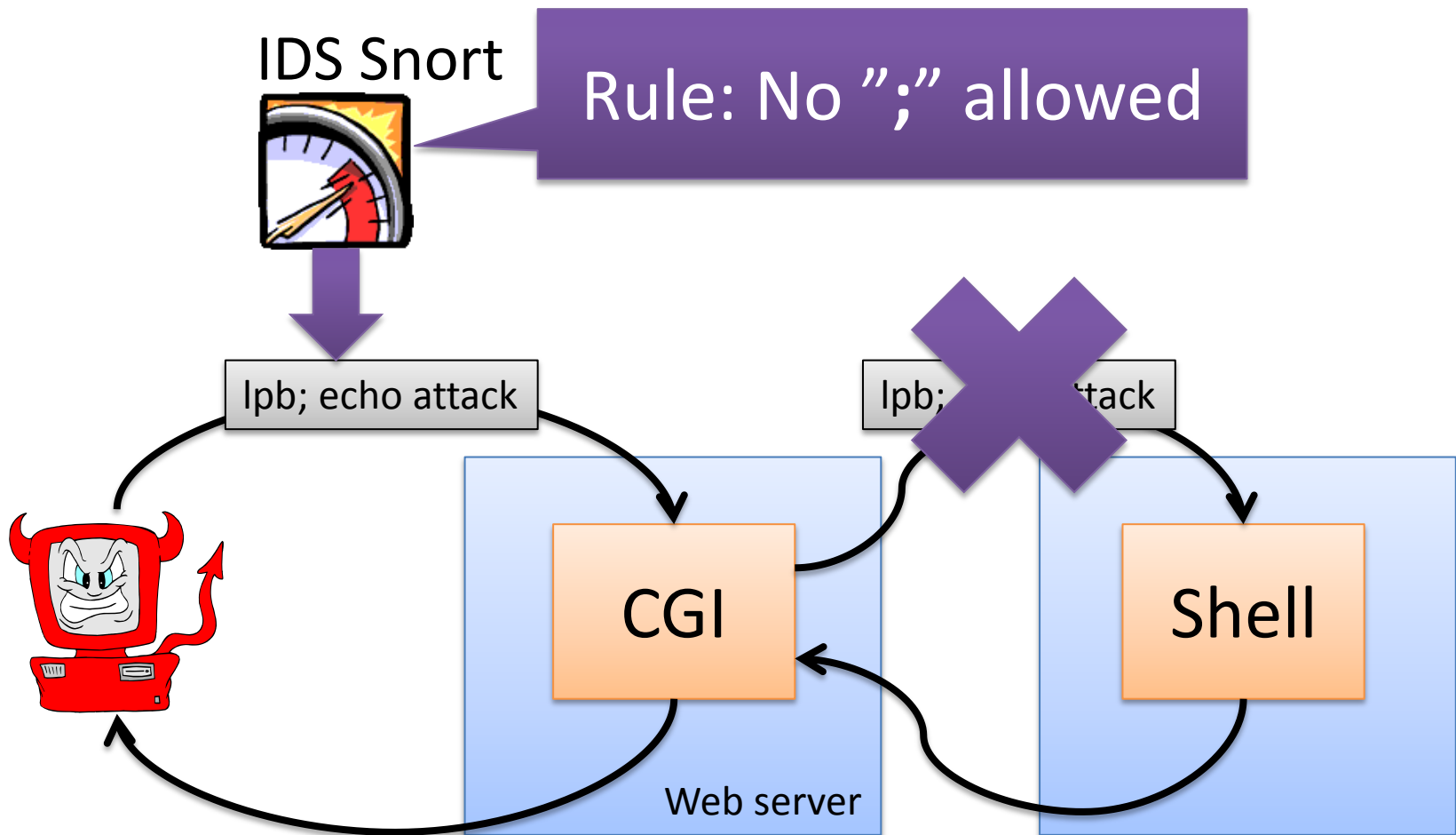
phf CGI Script fails to guard against newline characters

- CGI script phf, exploited late 1990's.
- Tried to sanitize input using a routine supplied in the web server
 - `escape_shell_cmd()`
 - Removing a number of shell meta characters BUT ...
 - Buggy: forgot to remove ***newline character***
- Attack:
embed a newline character in the string passed to the CGI script phf, resulting in additional commands to execute.

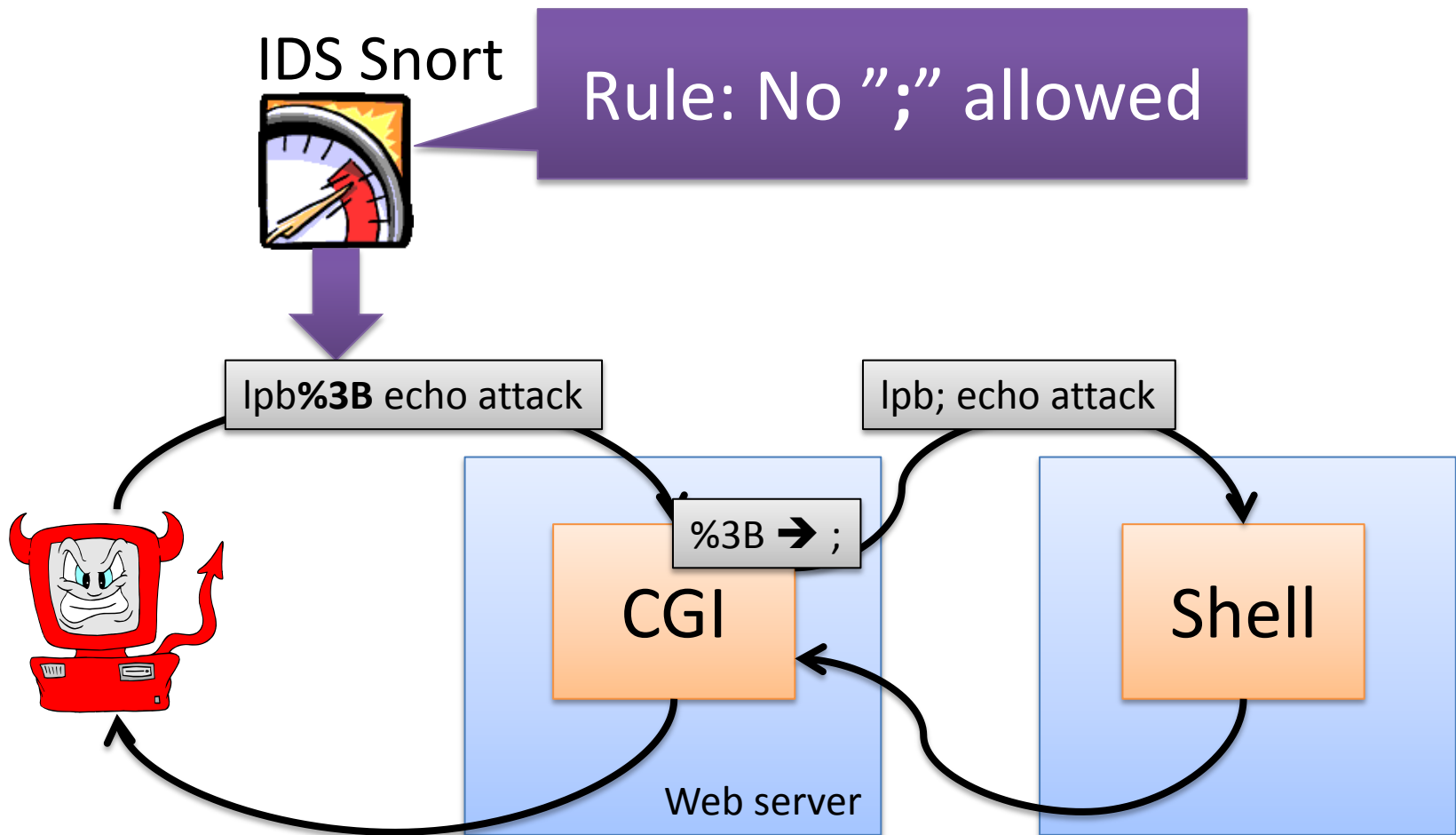
Example: Command Injection



Example: Command Injection



Example: Command Injection



OWASP

- The Open Web Application Security Project (OWASP) is ... organization focused on improving the security of application software.
- OWASP Local Chapter in Gothenburg
 - <https://www.owasp.org/index.php/Gothenburg>

OWASP Top 10 2010

- A1-Injection
- A2-Cross Site Scripting (XSS)
- A3-Broken Authentication and Session Management
- A4-Insecure Direct Object References
- A5-Cross Site Request Forgery (CSRF)
- A6-Security Misconfiguration
- A7-Insecure Cryptographic Storage
- A8-Failure to Restrict URL Access
- A9-Insufficient Transport Layer Protection
- A10-Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Top_10_2010-Main

<http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf>

OWASP Top 10 2010

Name	Description
A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
A2-Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites
A3-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.



SQL injection example

Courtesy of John Smith, IBM Cooperation, GB

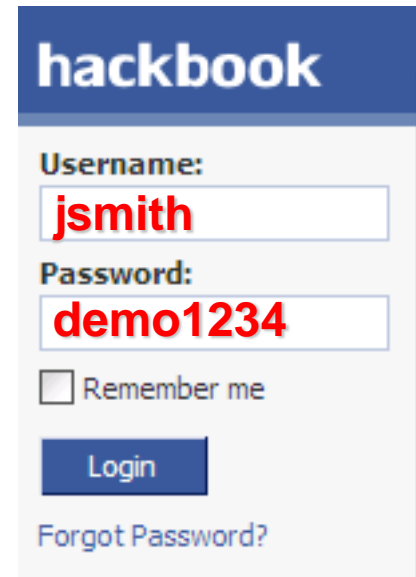
Injection Flaws

- ▶ What is it?
 - User-supplied data is sent to an interpreter as part of a command, query or data.
- ▶ What are the implications?
 - SQL Injection – Access/modify data in DB
 - SSI Injection – Execute commands on server and access sensitive data
 - LDAP Injection – Bypass authentication
 - ...

SQL Injection

User input is embedded as-is in predefined SQL statements:

```
query = "SELECT * from tUsers where  
        userid='" + iUserID + "' AND  
        password='" + iPassword + "'";
```



The screenshot shows a login interface for a site called 'hackbook'. It has a blue header with the site name. Below it, there are input fields for 'Username:' and 'Password:'. The username field contains 'jsmith' and the password field contains 'demo1234', both in red text. There is a checkbox labeled 'Remember me' and a blue 'Login' button. A link for 'Forgot Password?' is at the bottom.



UserID	Username	Password	Name
1824	jsmith	demo1234	John Smith

- Hacker supplies input that modifies the original SQL statement, for example: `iUserID = ' or 1=1 --`

```
SELECT * from tUsers where  
        userid='' or 1=1 -- ' AND password='bar'
```

SQL Injection

User input is embedded as-is in predefined SQL statements:

```
query = "SELECT * from tUsers where  
        userid='" + iUserID + "' AND  
        password='" + iPassword + "'";
```

hackbook

Username:

Password:

☐ Remember me

[Forgot Password?](#)



UserID	Username	Password	Name
1824	jsmith	demo1234	John Smith

- Hacker supplies input that modifies the original SQL statement, for example: `iUserID = ' or 1=1 --`



UserID	Username	Password	Name
1	admin	\$#kaoeFor	Admin

Summary

- ▶ Common theme with web application vulnerabilities:
 - Unvalidated user input is the attack vector
- ▶ Good security practice:
 - Assume all user input is evil !

OWASP Top 10 2010

Name	Description
A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.
A2-Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites
A3-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

Google Gruyere

Web Application Exploits and Defenses

- Want to beat the hackers at their own game?
 - Learn how hackers find security vulnerabilities!
 - Learn how hackers exploit web applications!
 - Learn how to stop them!
- <http://google-gruyere.appspot.com/.../>
- Example
 - XSS attack: same origin policy
 - Injected code stored at site – run when user visits site (or tricking user to click on URL in email)
 - Here is an image of a cute
`<a href="http://google-gruyere.appspot.com/.../
<script>alert(1)</script>">cat`



Web Application Exploits and Defenses

A Codelab by Bruce Leban, Mugdha Bendre, and Parisa Tabriz

UPDATED July 13, 2010: We have changed the name of the codelab application to Gruyere and have moved the location to this page. Please update your bookmarks.

Want to beat the hackers at their own game?

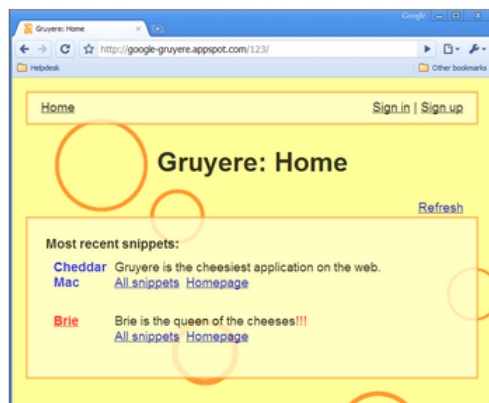
- Learn how hackers find security vulnerabilities!
- Learn how hackers exploit web applications!
- Learn how to stop them!

This codelab shows how web application vulnerabilities can be exploited and how to defend against these attacks. The best way to learn things is by doing, so you'll get a chance to do some real penetration testing, actually exploiting a real application. Specifically, you'll learn the following:

- How an application can be attacked using common web security vulnerabilities, like cross-site scripting vulnerabilities (XSS) and cross-site request forgery (XSRF).
- How to find, fix, and avoid these common vulnerabilities and other bugs that have a security impact, such as denial-of-service, information disclosure, or remote code execution.

To get the most out of this lab, you should have some familiarity with how a web application works (e.g., general knowledge of HTML, templates, cookies, AJAX, etc.).

Gruyere



This codelab is built around **Gruyere** /gru:ˈjɛər/ - a small, cheesy web application that allows its users to publish snippets of text and store assorted files. "Unfortunately," Gruyere has multiple security bugs ranging from cross-site scripting and cross-site request forgery, to information disclosure, denial of service, and remote code execution. The goal of this codelab is to guide you through discovering some of these bugs and learning ways to fix them both in Gruyere and in general.

The codelab is organized by types of vulnerabilities. In each section, you'll find a brief description of a vulnerability and a task to find an instance of that vulnerability in Gruyere. Your job is to play the role of a malicious hacker and find and exploit the security bugs. In this codelab, you'll use both black-box hacking and white-box hacking. In **black box hacking**, you try to find security bugs by experimenting with the application and manipulating input fields and URL parameters, trying to cause application errors, and looking at the HTTP requests and responses to guess server behavior. You do not have access to the source code, although understanding how to view source and being able to view http headers (as you can in Chrome or LiveHTTPHeaders for Firefox) is valuable. Using a web proxy like [Burp](#) or [WebScarab](#) may be helpful in creating or modifying requests. In **white-box hacking**, you have access to the source code and can use automated or manual analysis to identify bugs. You can treat Gruyere as if it's open source: you can read through the source code to try to find bugs. Gruyere is written in Python, so some familiarity with Python can be helpful. However, the security vulnerabilities covered are not Python-specific and you can do most of the lab without even looking at the code. You can run a local instance of Gruyere to assist in your hacking: for example, you can create an administrator account on your local instance to learn how administrative features work and then apply that knowledge to the instance you want to hack. Security researchers use both hacking techniques, often in combination, in real life.

We'll tag each challenge to indicate which techniques are required to solve them:



Challenges that can be solved just by using black box techniques.



Challenges that require that you look at the Gruyere source code.



Challenges that require some specific knowledge of Gruyere that will be given in the first hint.

WARNING: Accessing or attacking a computer system without authorization is illegal in many jurisdictions. While doing this codelab, you are specifically granted authorization to attack the Gruyere application as directed. You may not attack Gruyere in ways other than described in this codelab, nor may you attack App Engine directly or any other Google service. You should use what you learn from the codelab to make your own applications more secure. You should not use it to attack any applications other than your own, and only do that with permission from the appropriate authorities (e.g., your company's security team).

[Home](#)

[Sign in](#) | [Sign up](#)

Gruyere: Home

[Refresh](#)

Most recent snippets:

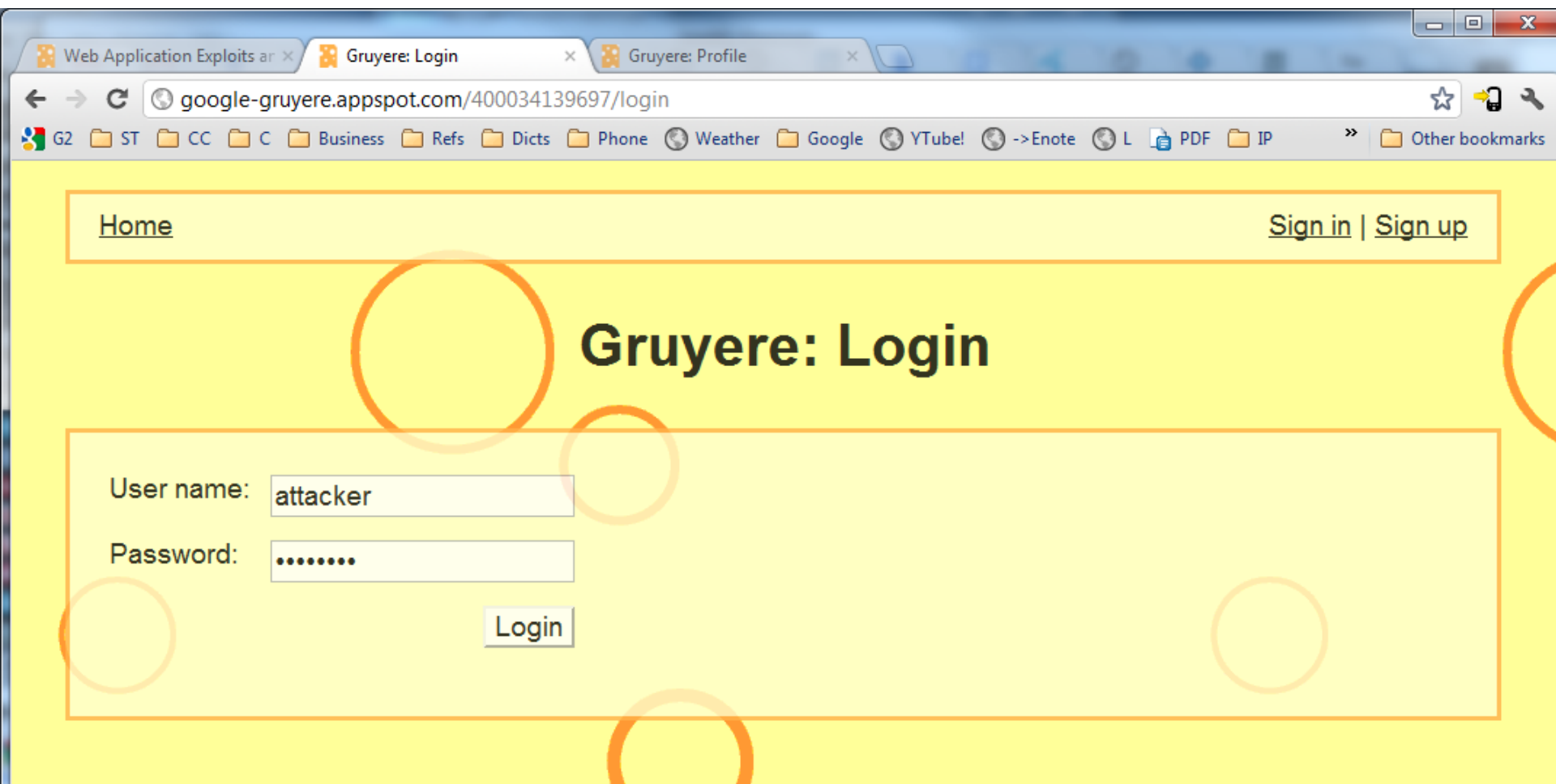
Cheddar Mac Gruyere is the cheesiest application on the web.
[All snippets](#) [Homepage](#)



attacker Do you know why garbage trucks drive so fast in Sweden? They are afraid of getting robbed...
[All snippets](#) [Homepage](#)

teacher All exam questions have been created!
[All snippets](#) [Homepage](#)

Brie Brie is the queen of the cheeses!!!
[All snippets](#) [Homepage](#)



[Home](#) | [My Snippets](#) | [New Snippet](#) | [Upload](#)

attacker <attacker> | [Profile](#) | [Sign Out](#)

Gruyere: New Snippet

Add a new snippet.

```
Here is an image of a cute <a href="http://google-
gruyere.appspot.com/400034139697/<script>alert(1)
</script>">cat</a>
```

Limited HTML is now supported in snippets (e.g., , <i>, etc.)!



Submit

[Home](#) | [My Snippets](#) | [New Snippet](#) | [Upload](#)

attacker <attacker> | [Profile](#) | [Sign out](#)

My Snippets

All snippets:

- 1  Here is an image of a cute [cat](#)
- 2  Do you know why garbage trucks drive so fast in Sweden? They are afraid of getting robbed

[My site](#)

[Home](#)

[Sign in](#) | [Sign up](#)

Gruyere: Login

User name:

Password:


Login

Gruyere: Home

[Refresh](#)

Most recent snippets:

Cheddar Mac Gruyere is the cheesiest application on the web.
[All snippets](#) [Homepage](#)

 **attacker** Here is an image of a cute [cat](#)
[All snippets](#) [Homepage](#)

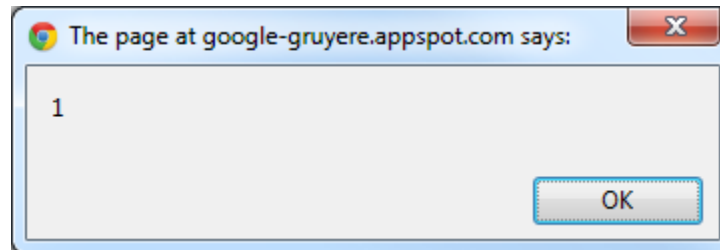
teacher All exam questions have been created!
[All snippets](#) [Homepage](#)

Brie Brie is the queen of the cheeses!!!
[All snippets](#) [Homepage](#)

[Home](#) | [My Snippets](#) | [New Snippet](#) | [Upload](#)

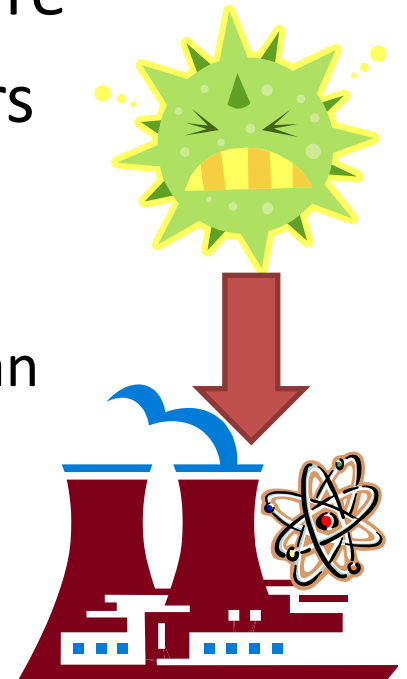
teacher <teacher> | [Profile](#) | [Sign Out](#)

Invalid request: /



New Era 2010: Stuxnet

- Advanced Malware
 - target specifically **P**rogrammable **L**ogic **C**ontrollers:
Siemens SIMATIC Step 7 software
 - Lots of rumors of goal and who creators
 - designed and released by a government
 - the U.S. or Israel ???
 - **Target:** Bushehr nuclear power plant in Iran
(60% of infected hosts in Iran)



Stuxnet: Pandora's box ?

- Stuxnet is advanced and one of the first wild malware's targeting PLCs.
 - 6—8 people about 6 months to create.
- PLCs exists in many industries
 - factory assembly lines, amusement rides, or lighting fixtures.



now blueprint to create malware targeting PLCs

- Compare this with the *Loveletter* virus (2000)
 - 2003/11 there existed 82 different variants of *Loveletter*.
 - It is claimed that more than 5,000 attacks are carried out every day.

Project Course: DAT285B

ICT Support for Adaptiveness and Security in the Smart Grid

CHALMERS GÖTEBORG UNIVERSITY
Computer Science and Engineering



ICT Support for Adaptiveness and Security in the Smart Grid DAT285B

Spring semester, study period 4, 2013

(DAT285 -- Masterclass in Areas of advance)

News:

- [2013-02-12] New draft home page created. Content will be added during February.

Course Description

Examiner:

- Associate Professor Marina Papatriantafyllou, phone: 031-772 5413, email: prianta
- Assistant Professor Magnus Almgren, phone: 031-772 1702, email: magnus.almgren

This is a masterclass in the area of advance, giving an overview of the smart grid and important technologies from the Information and Communication Technologies (ICT) area that is being used. The focus is on algorithms, distributed computing, communication and security.

In Europe and elsewhere, the electrical grid is being transitioned into the "smart grid" in order to increase flexibility and accommodate large scale energy production from renewable sources. This transition involves, among other steps, the installation of new, advanced equipment - for example, the replacement of traditional domestic electrical meters with smart meters - and remote communication with devices - for example, allowing remote access to an unsupervised energy production site.

The course is built around seminars where you learn about the design or development of systems, infrastructure, and applications that are related to the electric power smart grid, with a focus on distributed algorithms and security. You are expected to give some presentations, as well as to participate actively in discussions. As part of the course, you are also expected to complete lab work, i.e. a significant project with relevance to the smart grid. In this way you will also gain experience at the front connecting research and education in the main domain overlapping two of the Areas of Advance, namely ICT and Energy.

Recommended text book

The course is built around seminars, lecture notes and research papers.

Course Memo

The Course memo summarizes relevant information of the course.

Reading Instructions

<http://www.cse.chalmers.se/edu/course/DAT285B/>

ICT Support for Adaptiveness and Security in the Smart Grid (DAT285B)

- Goals
 - Letting students from computer science and other disciplines be introduced to advanced interdisciplinary concepts related to the smart grid, thus
 - building an understanding of the vocabulary and important terms that may have different meanings in the individual disciplines, and
 - investigating a domain-specific problem relevant to the smart grid that need an understanding beyond the traditional ICT field.

Two instances of DAT285

- LP2 = Autonomous and Cooperative Vehicular Systems
- *LP4 = ICT Support for Adaptiveness and Security in the Smart Grid*

Environment

- Based on both the present and future design of the smart grid.
 - How can techniques from distributed systems be applied to large, heterogeneous systems where a massive amount of data will be collected?
 - How can such a system, containing legacy components with no security primitives, be made secure when the communication is added by interconnecting the systems?
- The students will have access to a hands-on lab, where they can run and test their design and code.

Course Setup

- The course is given on an advanced master's level, resulting in 7.5 points.
- The course setup
 - The first part of the course consists of lectures to introduce the students to each other and the two disciplines (“crash course”).
 - The second part of the course will follow a seminar-style where research papers from both disciplines are actively discussed and then presented.
 - At the end of the course the students are also expected to present their respective project.