

Command Injection Attacks

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Command Injection Attacks

- A class of attacks in which

... data provided by the user

... is passed to an application

... which interprets

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

SQL Injection

User

Password

Assignment Project Exam Help

```
$query = "SELECT * FROM users WHERE user = '$_POST[user]' AND password = '$_POST[password]'"
```

<https://eduassistpro.github.io/>

```
$query = "SELECT * FROM users WHERE user = 'yveAR' AND password = '1=1;--'"
```

Add WeChat [edu_assist_pro](#)

A More Realistic Example

User

Password

Assignment Project Exam Help

```
$stmt = $db->query($sql);  
if ($row = $stmt->fetch(PDO::FETCH_ASSOC)) {  
    if (!password_match($row['password'], $password)) {  
        // ...  
    }  
}
```

<https://eduassistpro.github.io/>

Add WeChat: edu_assist_pro



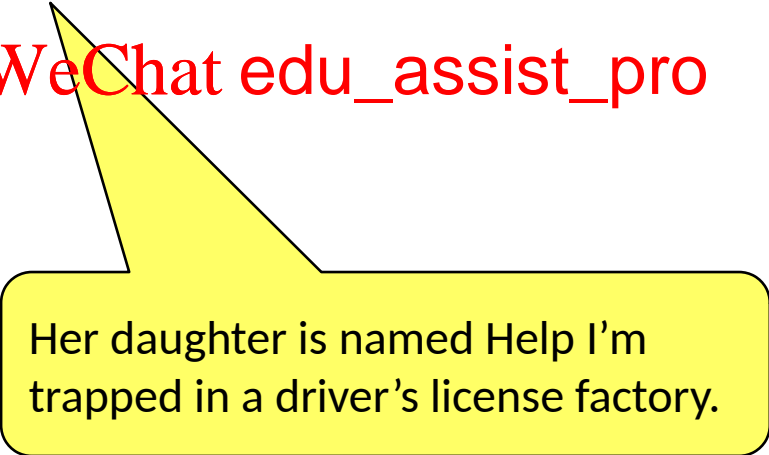
```
$query = "SELECT * FROM users WHERE user_id=' ' UNION  
SELECT 'admin', '$2a$05$b...'; --";
```

Exploits of a Mom

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro



Her daughter is named Help I'm trapped in a driver's license factory.

Injection Mechanisms

- User Input
- Server Variables

Assignment Project Exam Help
<https://eduassistpro.github.io/>
Add WeChat edu_assist_pro

```
function ip_addr() {  
  if (isset($_SERVER['REMOTE_ADDR'])) {  
    $ip_addr = $_SERVER['REMOTE_ADDR'];  
  } else {  
    $ip_addr = $_SERVER['REMOTE_ADDR'];  
  }  
}
```

```
$query = "SELECT FROM badHosts WHERE ip='".ip_addr().'" "
```

- Cookies

Another example

```
<?php
$name=$_GET['name'];
if (isset($name)) {
    echo "Hello $name",
}
?>
```

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

```
http://mysite.com/hello.php?n
%3Cscript%3Ealert%28%27XSS%27%29%3B%3C%2Fscript
%3E
```



Hello <script>alert('XSS');</script>

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Shell Injection

```
int main(int argc, char** argv) {  
    char cmd[CMD_MAX] = "/bin/cat";  
    strcat(cmd, a  
    system(cmd);  
}  
  
./program "/dev/null; ls"
```

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Attacking the Washington, D.C. Internet Voting System

Wolchok et al. FC 2012

run("gpg", "--trust-model always -o
\"#{File.expand_path(src.pa e -r
\"#{@recipient} https://eduassistpro.github.io/
\"#{File.expand_path(src.pa
Add WeChat edu_assist_pro

Upload file: **foo.\$ (cat ~/.bash_history)**

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Mitigation

- **Whitelist** –
 - Look for patterns that demonstrate that the data is valid. Reject everything else

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Whitelisting example

Assignment Project Exam Help

```
public boolean is
```

```
if (in == null https://eduassistpro.github.io/
```

```
return false;
```

```
if (Pattern.matches("^\d{5}" Add WeChat edu\_assist\_pro, in))
```

```
return true;
```

```
return false;
```

```
}
```

Whitelisting example

Assignment Project Exam Help

<https://eduassistpro.github.io/>

```
if (isValidZip(request.getParameter("zip")) == false) {  
    return response.BAD_ZIP;  
}
```

```
// parameter contains ZIP code, continue
```

```
show_zip = "<em>" + request.getParameter("zip") + "</em>";
```


Mitigation

- **Whitelist –**

- Look for patterns that demonstrate that the data is valid. Reject everything else
- Do you know the format of the input?
 - What characters can

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Class Exercise

- What is the format of an email address?

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Mitigation

- **Whitelist** –

- Look for patterns that demonstrate that the data is valid. Reject everything else
- Do you know the format of the input?
 - What characters can

- **Blacklist**

- Look for patterns that demonstrate that the data is invalid. Everything else is valid.
- Are you aware of all possible attacks?

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat [edu_assist_pro](#)

Blacklisting example

```
public boolean dontXSSmeBro(String in) {  
    if (in == null )  
        return false;  
    if (Pattern.matches("<script>$", in))  
        return false;  
    return true;  
}
```

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

The Samy Worm

- A MySpace worm developed in late 2005
- Uses XSS for self-reproduction
- When a user visits an infected profile
 - Add the worm's <https://eduassistpro.github.io/>
 - Add the worm to the visitor My
- The fastest spreading virus o according to Wikipedia)
 - More than 1,000,000 infections in 20 hours

As Samy tells it

- **10/04, 12:34 pm:** You have **73** friends.
- **1 hour later, 1:30 am:** You have **73** friends and **1** friend request.
- **7 hours later, 8:35 am:** You have **74** friends and **221** friend requests.
- **1 hour later, 9:30 am:** You have **74** friends and **480** friend requests.
 - Oh wait, it's exponential
- **1 hour later, 10:30 a** friend requests.
- **3 hours later, 1:30 pm:** You have **2,503** friend requests.
- **5 hours later, 6:20 pm:** I timidly go to my profile to view the friend requests. **2,503** friends. **917,084** friend requests.
 - I refresh three seconds later. **918,268**. I refresh three seconds later. **919,664** (screenshot below). A few minutes later, I refresh. **1,005,831**.

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat [edu_assist_pro](https://eduassistpro)

Technical info 1

1. Myspace blocks a lot of tags. In fact, they only seem to allow <a>, s, and <div>s...maybe a few others (<embed>'s, I think)...
 - However, some browsers allow javascript within CSS tags.
 - **Example:** `<div style="background:url(javascript:alert(1))">`
3. However, myspace strips out the "cript" from ANYWHERE.
 - Some browsers will actually interpret "java\nscript" as "javascript"
 - **Example:**
`<div id="mycode" expr="alert('hah!')" style="background:url('java script:eval(document.all.mycode.expr)')">`

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Technical info 2

4. Myspace got me...they STRIP OUT all escaped quotes

- We can just convert decimal to ASCII in javascript

- **Example:**

```
<div id="mycode" expr="alert('double quote: ' +  
String.fromCharCode(0x00000000):url('java  
script:eval(docu
```

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

5. Myspace gets me again and strips out "innerHTML" anywhere.

- We use an eval() to evaluate two strings and put them together to form "innerHTML".
- **Example:** alert(eval('document.body.inne' + 'rHTML'));

Mitigation

- **Whitelist –**

- Look for patterns that demonstrate that the data is valid. Reject everything else
- Do you know the format of the input?
 - What characters can

- **Blacklist**

- Look for patterns that demonstrate that the data is invalid. Everything else is valid.
- Are you aware of all possible attacks?

- **Quoting**

- Transform data to ensure safety
- Many times is easier said than done

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Quoting

- Protect special characters

```
$txt=preg_replace("/&/", "&amp;", $txt);  
$txt=preg_replace("/</", "&lt;", $txt);  
$txt=preg_replace("/>/", "&gt;", $txt);  
$txt=preg_replace("/\"/\"", $txt);  
echo $txt
```

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

System quoting code

- HTML escaping:

- PHP: `htmlspecialchars`

- CGI: `Html::Entities`

- Python: `cgi.escape`

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Prepared Statements

- Wrong

```
def add(table,*args):  
    statement="INSERT INTO %s VALUES %s"%args  
    cursor.execu
```

Assignment Project Exam Help

<https://eduassistpro.github.io/>

- Right

```
def add(table,*args):  
    statement="INSERT INTO table VALUES ?"  
    cursor.execute(statement, args)
```

Add WeChat edu_assist_pro

However

- Not always wanted
 - May want to allow some HTML tags
- Does not always
 - <https://eduassistpro.github.io/>
 - "Apparently javascript's URL-escape() function doesn't escape everything" [Add WeChat edu_assist_pro](#)
 - Second Order SQL Injection
 - ShellShock / ImageTragick

Other approaches

- Encrypt sensitive data

- Automatic tainting

- Apache::TaintRequest

- Secure language

- Microsoft LINQ

```
var q = from c in db.Cu
        where c.City == "Austin"
        select c.ContactName;
```

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat: edu_assist_pro

Summary

- Untrustworthy (non-controlled) input that goes into dynamic string building is a problem
- Apply as much input validation as you can
- Prefer whitelisting to blacklisting when possible and appropriate
- Sanitize output before presentation layer (browser, etc.)
- Use parametrization whenever possible, not convenience)
- When everything else fails, quote and escape
- **You will get things wrong!!!**

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro