Command Injection Attacks

Command Injection Attacks

- A class of attacks in which
  - … data provided by the user
  - … is passed to an application
  - … which interprets it as commands

VOTER RECORDS COPIED OFF COMPROMISED ILLINOIS VOTER REGISTRY

STOLEN CREDENTIALS: SOFTWARE VULNERABILITY

The Illinois State Board of Elections online voter registration has been hacked.

"The attackers took advantage of a programming flaw in the website's database. The attack, known as a 'SQL injection,' occurs in databases using the SQL programming language," the Hill explains.

Unless properly configured, SQL databases can be tricked into running commands entered by any website visitor.

SQL Injection

User 'yvOR 1=1;--

Password secret


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



```
$query = "SELECT * FROM users WHERE user_id='yvOR'1=1;--'
          AND password='secret'"
```

A More Realistic Example

User: ' UNION SELECT 'admin','$2a$05$b

Password:


```
$query = "SELECT * FROM users WHERE user_id='$_POST[user]'";
$stmt = $db->query($query);
$row = $stmt->fetch(PDO::FETCH_ASSOC);
if (!password_match($_POST['password'], $row['password']) {
    . . .
}
```



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

Exploits of a Mom

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

Injection Mechanisms

- User Input
- Server Variables


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

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

- Cookies

Another example

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



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

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

eBay, 2014

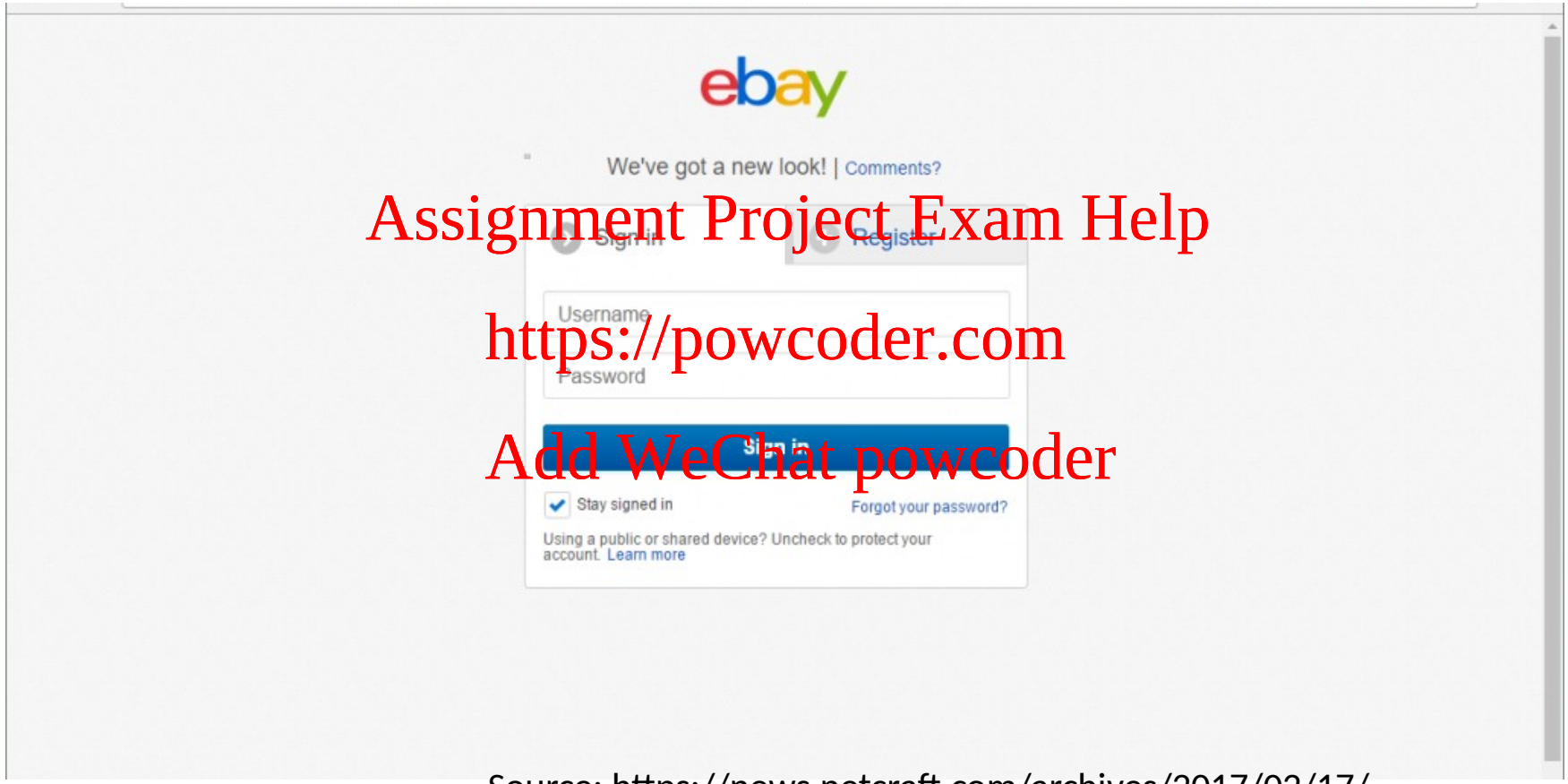
EBay: Another Security Breach

Earlier in 2014, we learned that eBay had been hacked, with millions of usernames and passwords potentially revealed to cyber criminals in a breach that the online auction service somehow failed to reveal for several months. The company is already facing a class action lawsuit in the USA concerning this event.

This week (just days after a seven hour outage hit sellers) researchers discovered that eBay security has been breached again, this time by manipulating the cross site scripting vulnerability, a weakness that should have been patched a long time ago.

Source: http://www.makeuseof.com/tag/ebay-security-breach-reconsider-membership/

eBay, 2017



Source: https://news.netcraft.com/archives/2017/02/17/hackers-still-exploiting-ebays-stored-xss-vulnerabilities-in-2017.html

Shell Injection

```
int main(int argc, char** argv) {
  char cmd[CMD_MAX] = "/bin/cat ";
  strcat(cmd, argv[1]);
  system(cmd);
}
```



```
./program "/dev/null; ls"
```

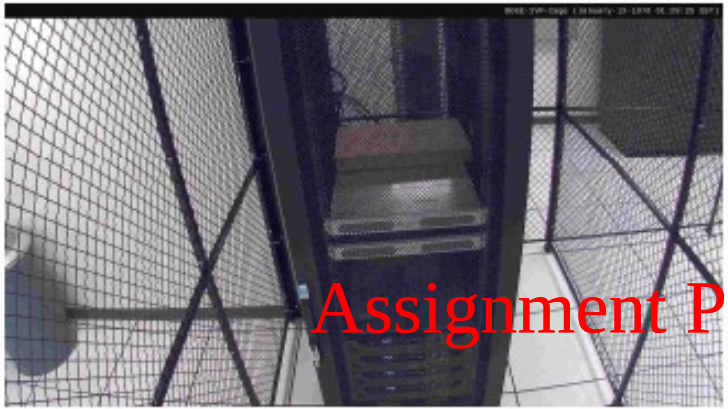

Adapted from: https://www.owasp.org/index.php/Command_Injection

Attacking the Washington, D.C. Internet Voting System

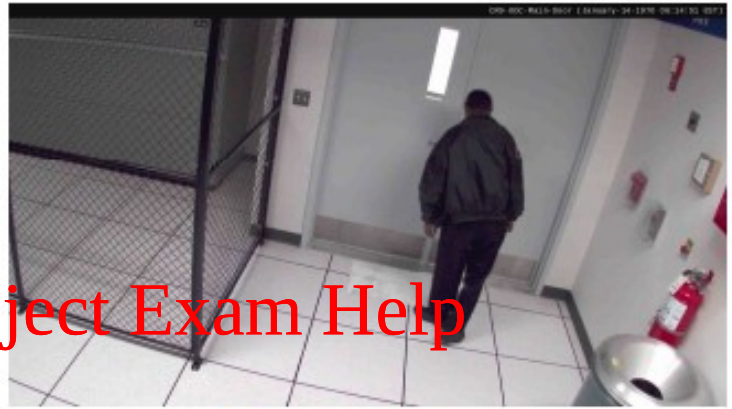
Wolchok et al. FC 2012

```
run("gpg", "--trust-model always -e
      \"#{File.expand_path(dst.path)}\" -e -r
      \"#{@recipient}\"
      \"#{File.expand_path(src.path)}\"")
```


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



(a) Voting server rack



(b) Security guard

(c) Typical workers, before attack

(d) Workers, after learning of attack

Source: Wolchok et al. FC 2012

Mitigation

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

Whitelisting example


```
public boolean isValidZip(String in) {
   if (in == null )
      return false;
   if (Pattern.matches("^\d{5}(-\d{4})?$", in))
      return true;
   return false;
}
```

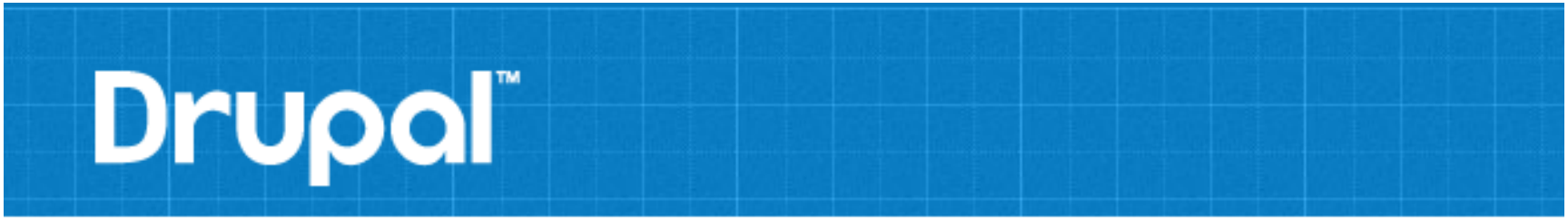
Whitelisting example


```
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 go into a name?



Download & Extend

Download & Extend Home | Drupal Core | Distributions | Modules | Themes

Fullname field for CCK » Issues

Name fields don't allow non-alpha characters

The Fullname field looks good, but when I try and enter a name with anything other than alpha characters (eg an apostrophe or a hyphen) it's rejected. So I can't enter my good friends Gavin O'Reilly and Mary-Jane Osborne-White :(

Source: https://www.drupal.org/node/129165

CHRISTOPHER NULL 11.05.15 5:26 AM

HELLO, I'M MR. NULL. MY NAME MAKES ME INVISIBLE TO COMPUTERS

PATRICK GEORGE/GETTY IMAGES

Source: http://www.wired.com/2015/11/null/

Class Exercise

- What is the format of an email address?

Email address – Local part

Local-part [edit]

The local-part of the email address may use any of these ASCII characters:

- uppercase and lowercase Latin letters `A` to `Z` and `a` to `z` ;
- digits `0` to `9` ;
- special characters `!#$%&'*+-/=?^_`{|}~` ;
- dot `.` , provided that it is not the first or last character unless quoted, and provided also that it does not appear consecutively unless quoted (e.g. `John..Doe@example.com` is not allowed but `"John..Doe"@example.com` is allowed);[5]
- space and `"(),:;<>@[\]` characters are allowed with restrictions (they are only allowed inside a quoted string, as described in the paragraph below, and in addition, a backslash or double-quote must be preceded by a backslash);
- comments are allowed with parentheses at either end of the local-part; e.g. `john.smith(comment)@example.com` and `(comment)john.smith@example.com` are both equivalent to `john.smith@example.com` .

Source: Wikipedia

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

Blacklisting example

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

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 author (Samy Kamkar) as a hero
  - Add the worm to the visitor MySpace profile
- The fastest spreading virus of all time (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, isn't it. Shit.
- **1 hour later, 10:30 am:** You have **518** friends and **561** friend requests.
- **3 hours later, 1:30 pm:** You have **2,503** friends and **6,373** 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**.

Extracted from: http://samy.pl/popular/

Technical info 1

1. Myspace blocks a lot of tags. In fact, they only seem to allow <a>, <img>s, and s...maybe a few others (<embed>'s, I think)...
   - However, some browsers allow javascript within CSS tags.
   - **Example**:

3. However, myspace strips out the word "javascript" 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)')">

Extracted from: https://samy.pl/popular/tech.html

Technical info 2

4. Myspace got me…they STRIP OUT all escaped quotes
   - We can just convert decimal to ASCII in javascript
   - **Example**:

5. Myspace gets me again and strips out the word "innerHTML" anywhere.
   - We use an eval() to evaluate two strings and put them together to form "innerHTML".
   - **Example**: alert(eval('document.body.inne' + 'rHTML'));

Extracted from: https://samy.pl/popular/tech.html

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 go into a name?
- 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

Quoting

- Protect special characters

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

System quoting code

- HTML escaping:
  - PHP: htmlentities
  - CGI: Html::Entities::encode
  - Python: cgi.escape

Prepared Statements

- Wrong

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


- Right

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

However

- Not always wanted
  - May want to allow some HTML tags
- Does not always work
  - "Apparently javascript's URL-encoding and escape() function doesn't escape everything necessary" – Samy Kamkar
  - Second Order SQL Injection
  - ShellShock / ImageTragick

Other approaches

- Encrypt sensitive data
- Automatic tainting
  - Apache::TaintRequest
- Secure language semantics
  - Microsoft LINQ


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

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 sending it over to the presentation layer (browser, etc.)
- Use parametrization whenever possible (by existence, not convenience)
- When everything else fails, quote and escape
- **You will get things wrong!!!**