RIA security based on OWASP Top 10

Kim Leppänen
Leif Åstrand

```
<script language=“javascript”>
if ( prompt("Enter password") == “supersecret" ) {
    document.location.href = "secret.html";
}
</script>
```

OWASP Top 10

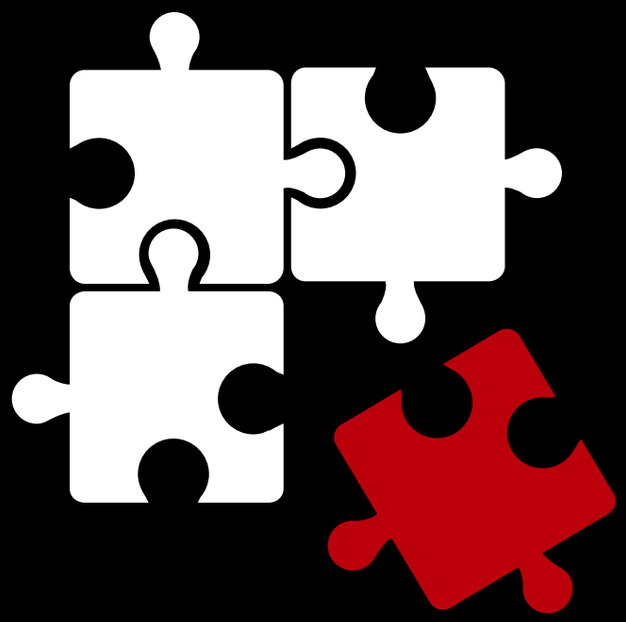
Open Web Application Security Project

vaadin }>

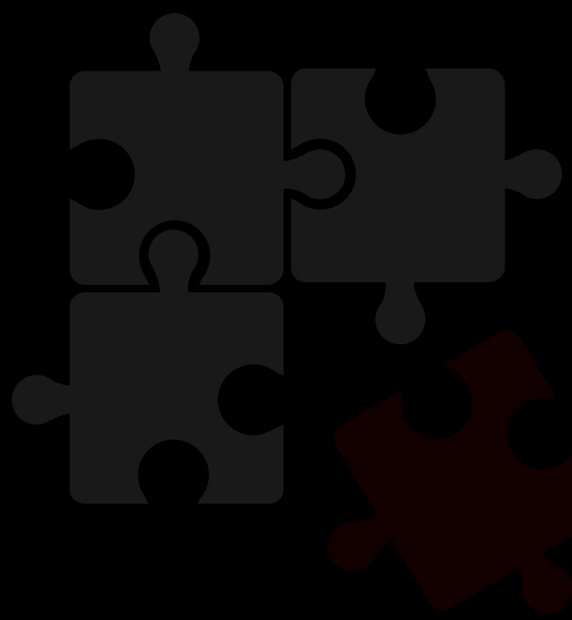
Rich Internet Applications

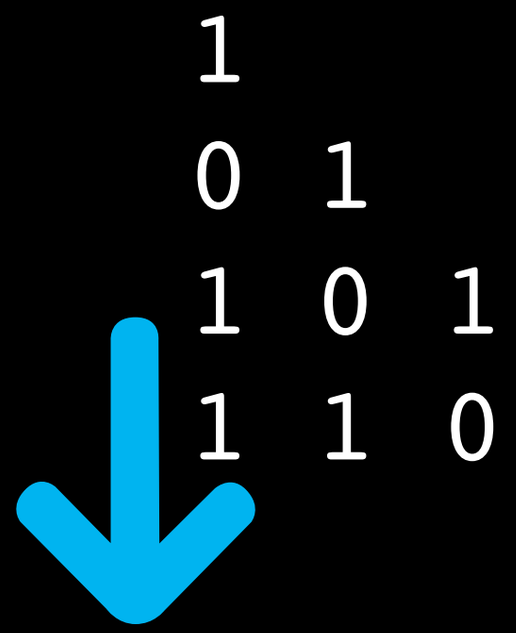
vaadin }>

vaadin }>



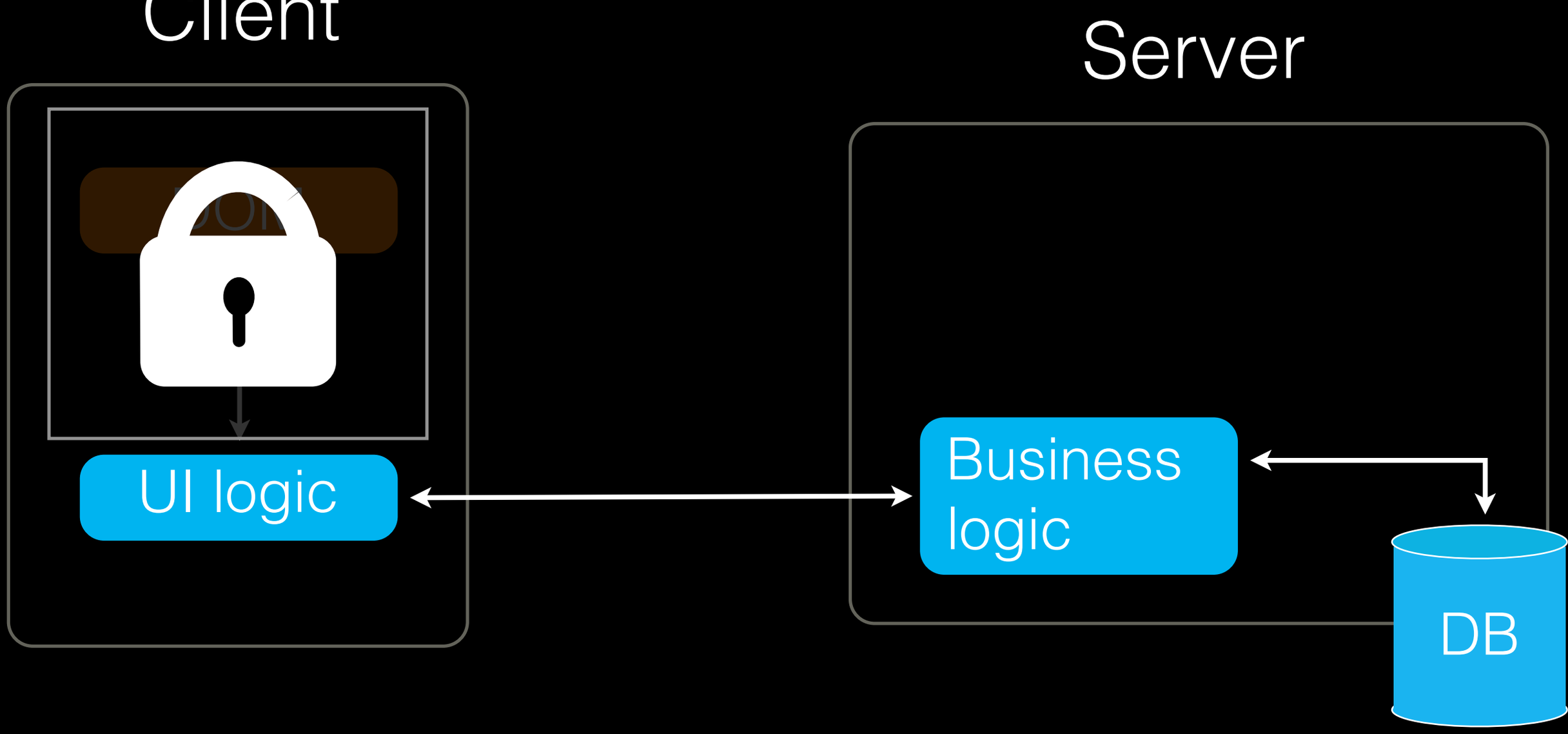
vaadin }>



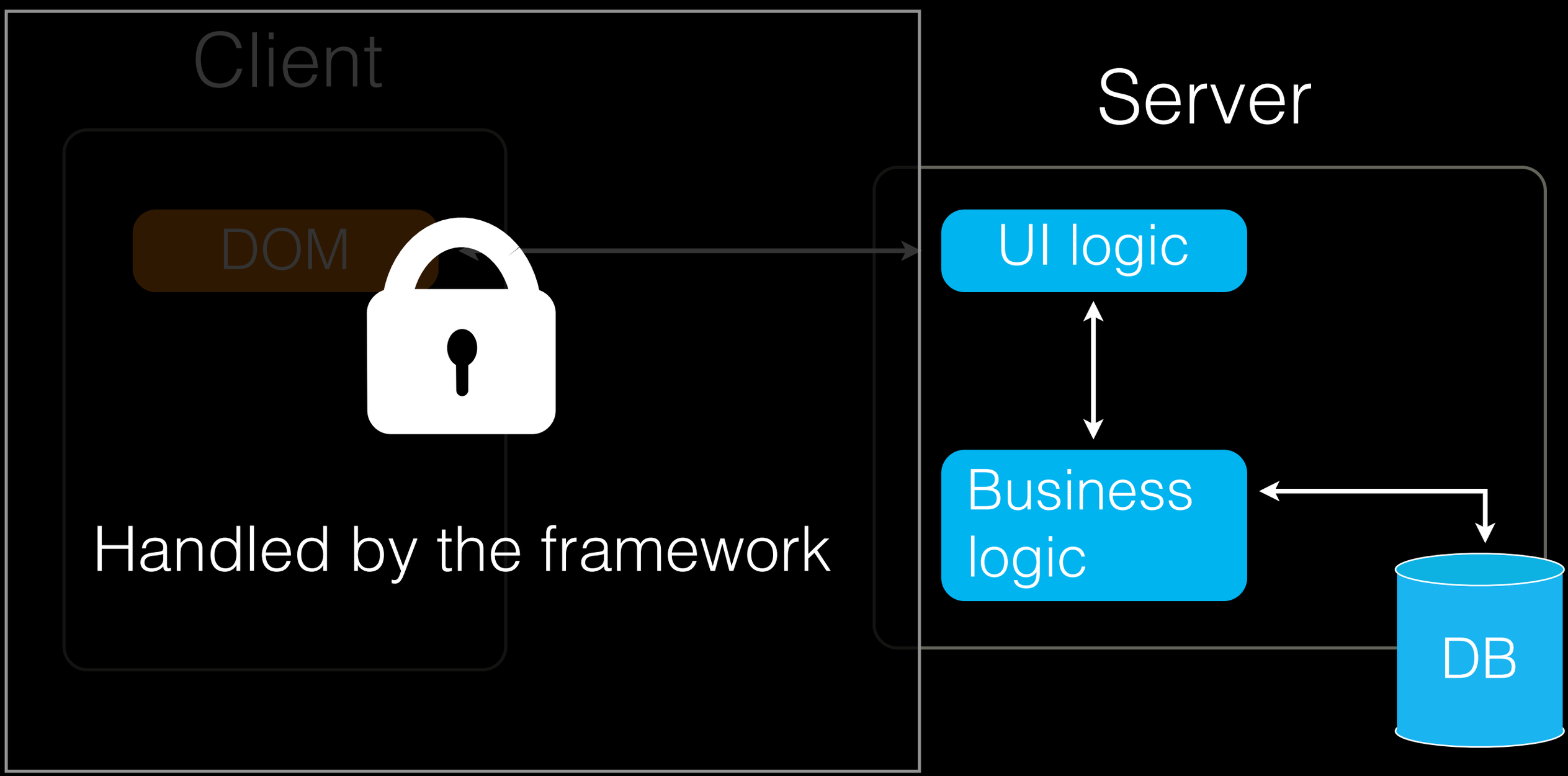


vaadin }>

GWT



Vaadin



vaadin }>

A1: Injection

vaadin }>

```
“SELECT * FROM Users WHERE username=’”
+ userNameField.getValue() + “’“
```

Not just SQL - could also be JPQL, HQL, shell, XPath, XML, LDAP, regex, eval, ...

Web frameworks can help

GWT

- N/A

Vaadin

- N/A

vaadin }>

A2: Broken Authentication and Session Management

vaadin }>

Session ID fixation

Exposure of session ID

Exposing user credentials

vaadin }>

Web frameworks can help

GWT

- N/A

Vaadin

- Helper for changing session id

A3: Cross-Site Scripting (XSS)

vaadin }>

Demo: auction application

vaadin }>

Web frameworks can help

GWT

- setText
- SafeHtml

Vaadin

- setHtmlContentAllowed(false)
- Beware of tooltips (setDescription)

Other things to keep in mind

- Consider using Markdown
- Context is king
- The XSS filter evasion cheat sheet

A4: Insecure Direct Object References

vaadin }>

Web frameworks can help

GWT

- Not so much, since this is mostly a server-side thing
- Can be hard to realize the problem since requests are “invisible”

Vaadin

- All ids are generated values that the server uses to find the right object when needed

A5: Security Misconfiguration

vaadin }>

Web frameworks can help

GWT

- N/A

Vaadin

- productionMode = true

A6: Sensitive Data Exposure

vaadin }>

Keep in mind

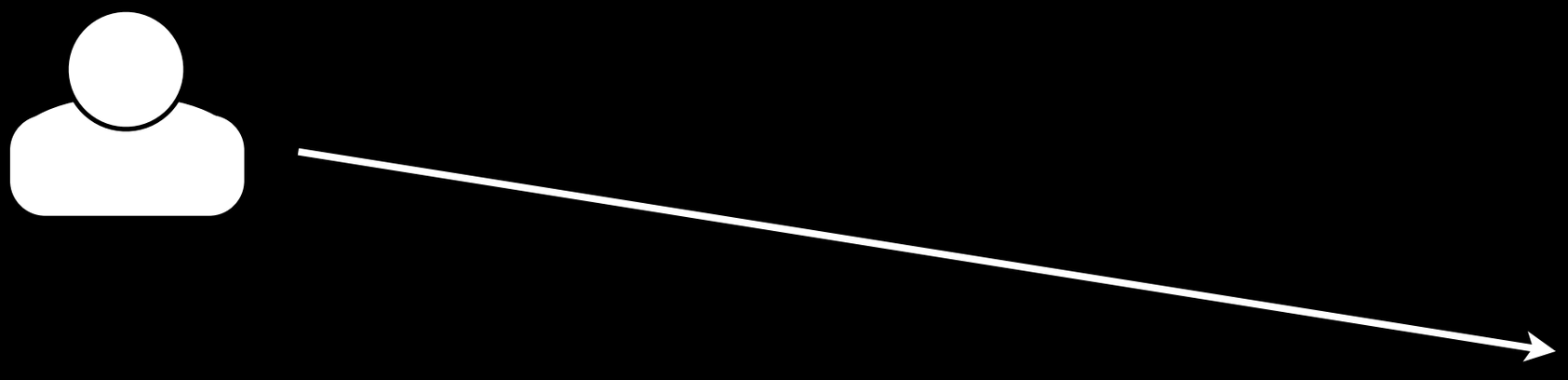
- Use SSL, no excuses!
- Salt and hash passwords
- Avoid handling sensitive data,
  e.g. credit card numbers

A7: Missing Function Level Access Control

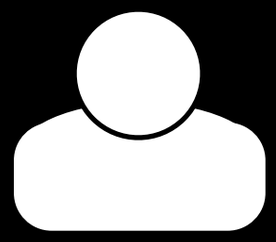
vaadin }>

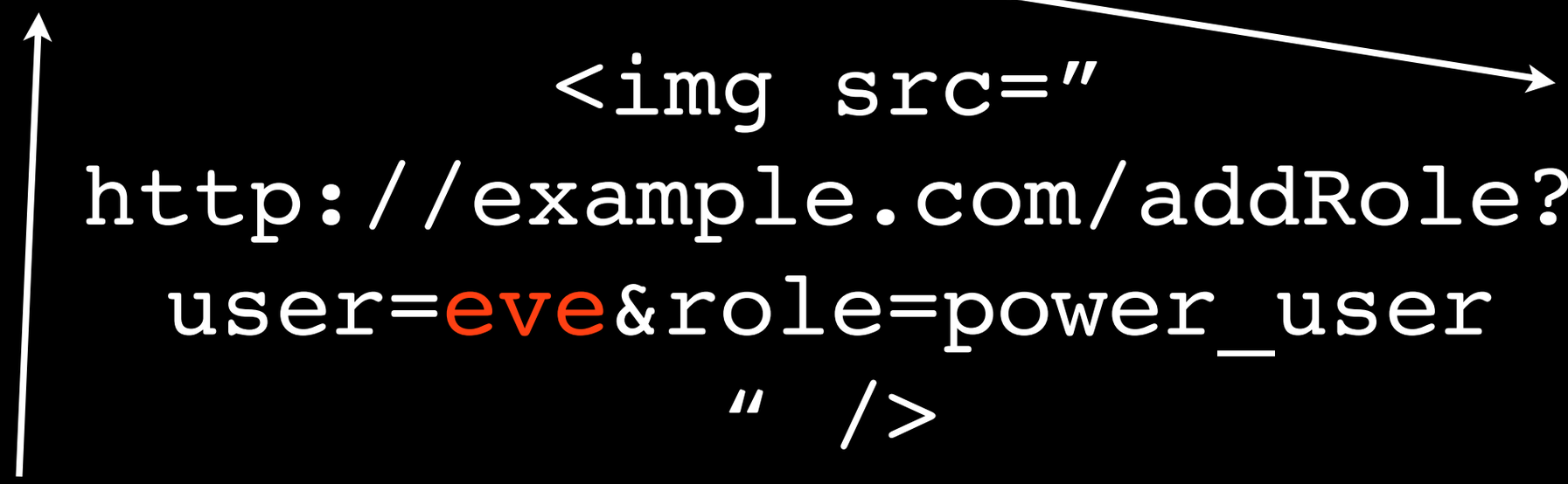
A8: Cross-Site Request Forgery (CSRF)

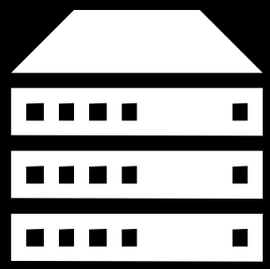
vaadin }>



```
http://example.com/addRole?
user=adam&role=power_user
```




<img src="
http://example.com/addRole?
user=eve&role=power_user
" />



```
http://example.com/addRole?
user=eve&role=power_user&token=abcd
```

Web frameworks can help

GWT

- GWT-RPC: XsrfTokenService and/or HasRpcToken
- RequestFactory: Make your own RequestTransport

Vaadin

- Secured out of the box

A9: Using Components with Known Vulnerabilities

vaadin }>

How do you know whether they are vulnerable?

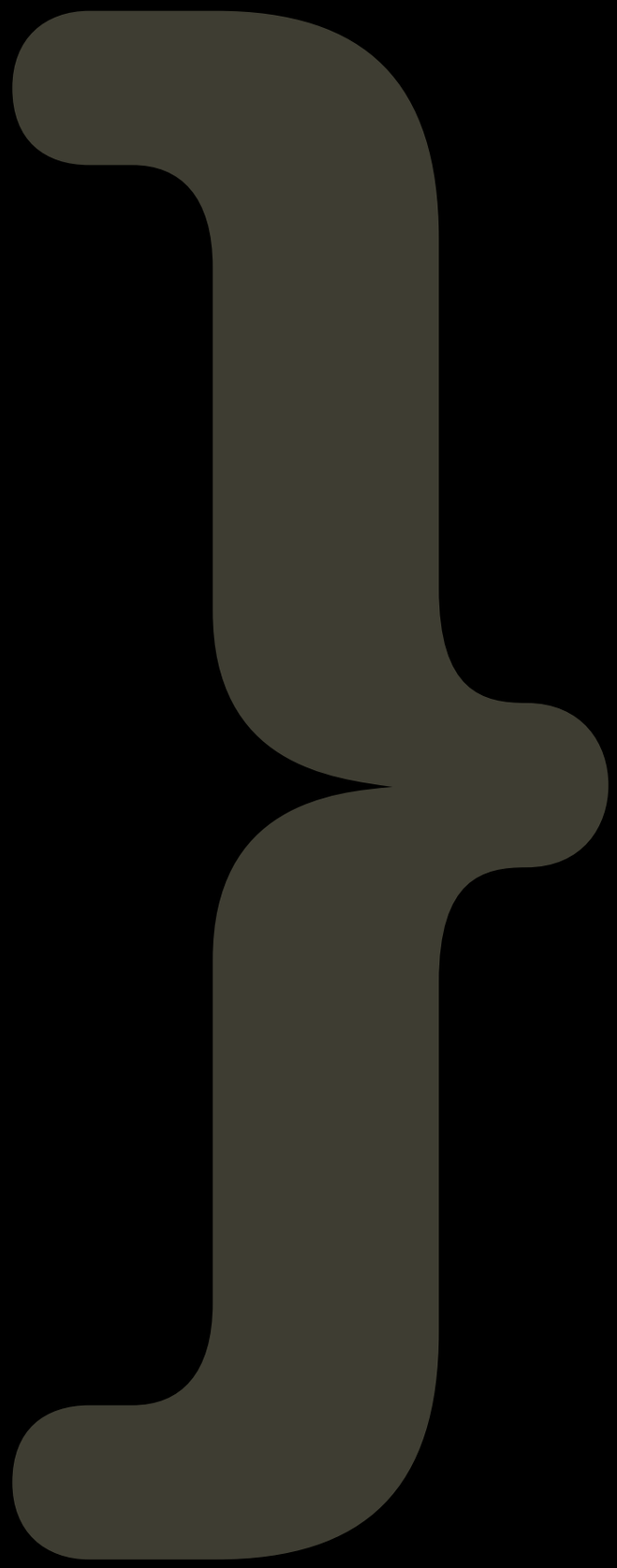
vaadin }>

A10: Unvalidated Redirects and Forwards

vaadin }>

```
<a href=”http://myapp.com?
redirect=example.com/evil"> Open app </a>
```

vaadin }>



Very quick conclusion

vaadin }>

Did we get some detail wrong?

Questions?

leif@vaadin.com
kim@vaadin.com

vaadin }>