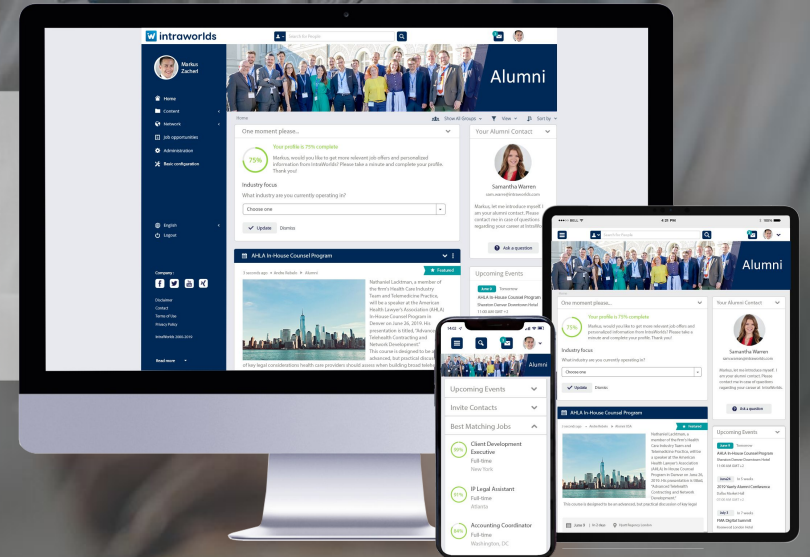


Web Application Security

WBU December 4th 2019



About IntraWorlds

IntraWorlds is a global provider of cloud-based talent relationship and alumni management software

- Established: 2002
- Employees: 50+
- Locations:



Munich



New York



Tampa



Pilsen



Clients 150+

IntraWorlds is proud to be a trusted partner of FORTUNE 1000 as well as leading law firms:

- Davis Polk
- Akin Gump
- Paul Hastings
- Sidley Austin
- Allen & Overy
- Mayer Brown
- White & Case
- Hogan Lovells



Internship



IWorkshop



Topics for Bachelor thesis



 <https://github.com/intraworlds/workshop-web-security>

ISO 27001

INFORMATION SECURITY MANAGEMENT SYSTEM

ISO 27001

ISMS

Human Resources
Access control
Cryptography
Physical and environmental security
Communications security
...
and many more

Development security

Coding standards, Security principles, Penetration testing

What's penetration testing?

OWASP

Open Web Application Security Project

<https://www.owasp.org>

OWASP top 10

List of most common security issues

Most common attacks on
the Web?

SQL Injection

(SQL) Injection

```
$sql = 'SELECT * FROM user WHERE id = ' . $_GET['id'];
```

demo

```
$sql = 'SELECT * FROM user WHERE id = :id';  
$stmt = $pdo->prepare($sql);  
$stmt->execute([':id' => $_GET['id']]);
```

XSS

Cross-site scripting

```
echo 'You are searching for ' . $_GET['query'];
```

demo

Self-retweeting tweet



*andy
@derGeruhn



+ Follow

```
<script  
class="xss">$($('.xss').parents().eq(1).find('a')  
.eq(1).click());$('[data-  
action=retweet]').click();alert('XSS in  
Tweetdeck')</script> ❤️
```

↩ Reply ↻ Retweet ★ Favorite ⋮ More

RETWEETS
83,502

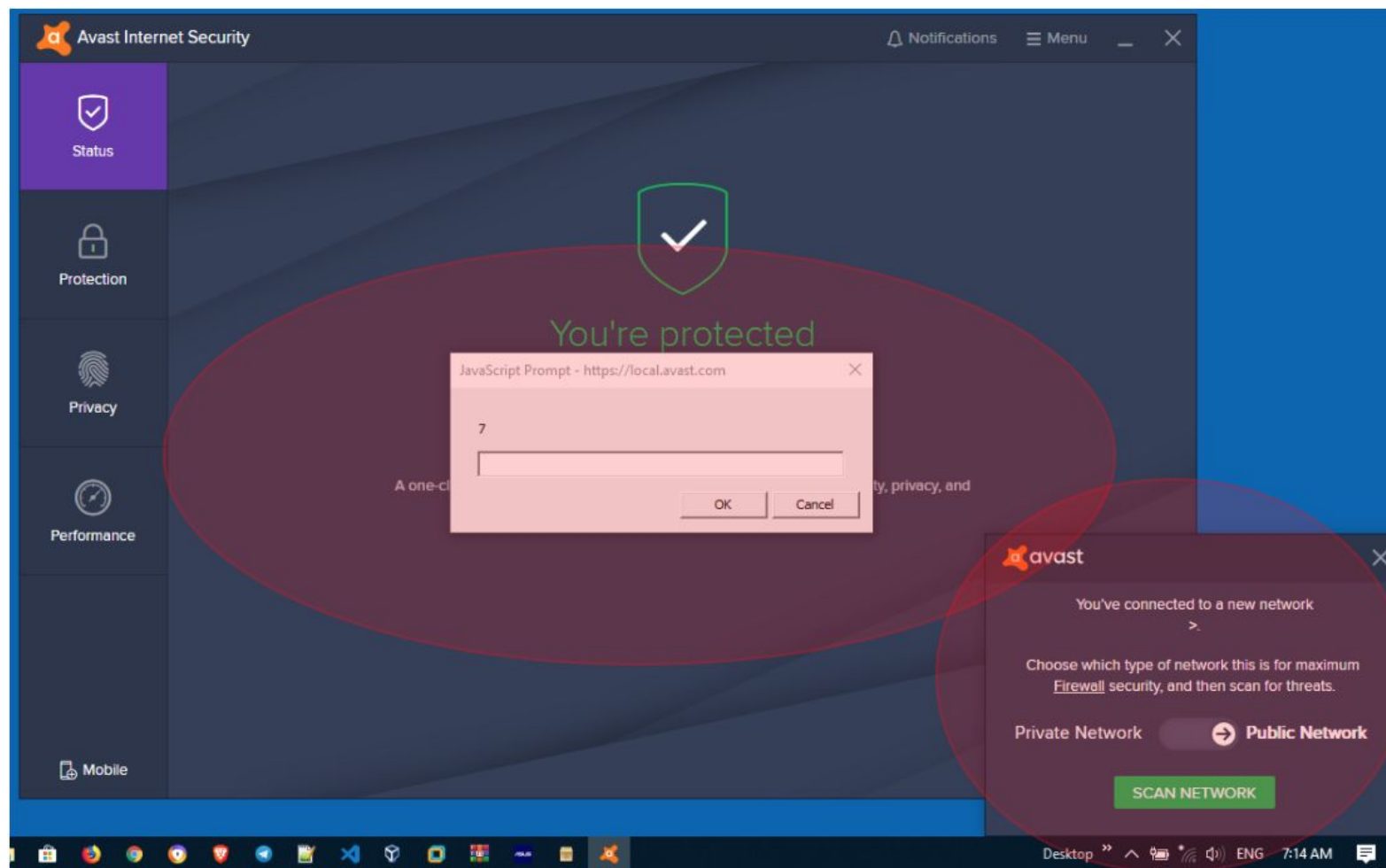
FAVORITES
9,709



9:36 AM - 11 Jun 2014

source: <https://www.zdnet.com/article/tweetdeck-wasnt-actually-hacked-and-everyone-was-silly/>

Avast AntiVirus Desktop XSS



source: <https://medium.com/bugbountywriteup/5-000-usd-xss-issue-at-avast-desktop-antivirus-for-windows-yes-desktop-1e99375f0968>

```
echo 'You are searching for ' . htmlspecialchars($_GET['query']);
```

CSP

Content-Security-Policy

CSRF

Cross-site request forgery

```
if ($isAuthenticated) payTo($_REQUEST['user_id']);
```

demo

```
$csrfMatches = $_SESSION['csrf'] == $_POST['csrf'];  
  
    if ($isAuthenticated && $csrfMatches)  
        payTo($_POST['user_id']);  
  
$_SESSION['csrf'] = bin2hex(random_bytes(16));
```

Directory Traversal

Directory Traversal

`https://example.com?download=../../../../etc/passwd`

demo

Sensitive data exposure

Sensitive data exposure

```
$password = md5( `APm9FK7Yn` );
```

demo

Security misconfigurations

Security misconfigurations

```
apt-get install mongodb  
service mongod start
```

XML External Entities (XXE)

Weak authentication and session management

Using Components with known vulnerabilities

Best practices

What's most important?
... in web security

Everything is user input
form data, files, headers

Implement with
frameworks/libraries
if possible
basic security out-of-the-box

Learn about security headers
browsers will prevent many attacks in the first place

Learn about secure
configuration
or use cloud

Learn about secure
configuration
or use cloud

Add CAPTCHA
on public pages
keep that pesky robots away

Use password manager
never reuse passwords

Use 2FA if possible
especially on github/gitlab, etc.

Use strong cryptography
bcrypt for passwords, SHA256 for hashing

Make a plan what to do in
case of security attack
you'll be hacked if successful



 <https://github.com/intraworlds/workshop-web-security>

 <https://facebook.com/intraworldscz/>