

Security Testing Course



W: www.sangbui.com

T: @sangsecurity

E: sangbuicom@gmail.com



OWASP

Open Web Application
Security Project



Agenda

- Introducing
- Security Mindset
- Intercept & Modify Request
- Hands on Labs : Bypass the client side validation
- Security Test Report



Security Mindset

Security Bug (Defect)



Security Mindset

~~Security Bug (Defect)~~

ERROR: The password you entered for the username **admin** is incorrect. [Lost your password?](#)

Username or Email Address

admin

Password

☐ Remember Me

Log In



Security Mindset

Security Risks

- **Risk is the potential** of gaining or losing something of value
- Can be gained or lost when taking risk resulting from a given action or inaction

WIKIPEDIA



Security Mindset

Even it is not a bug, but it still a risk

Risk = likelihood x impact

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Info	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			



Security Mindset

An application should respond with a *generic error message* regardless of whether the user ID or password was incorrect.

ERROR: The password you entered for the username **admin** is incorrect. [Lost your password?](#)

Username or Email Address

Password

☐ Remember Me



Security Mindset

An application should respond with a *generic error message* regardless of whether the user ID or password was incorrect.

The screenshot shows the HackerOne sign-in interface. At the top, a dark grey header contains a yellow error message box with the text "Invalid email or password." and a close icon. Below this, the main content area is light grey and features the title "Sign in to HackerOne". The sign-in form is a white box with a light blue border. It contains two input fields: "Email address" (highlighted in yellow) and "Password" (with a toggle icon). Below the email field is a link "Using SAML? Email address only, no password needed.". Below the password field is a checkbox "Remember me for two weeks" and a link "Forgot your password?". At the bottom of the form is a green "Sign in" button.

Invalid email or password. ✕

Sign in to HackerOne

Email address

Using SAML? Email address only, no password needed.

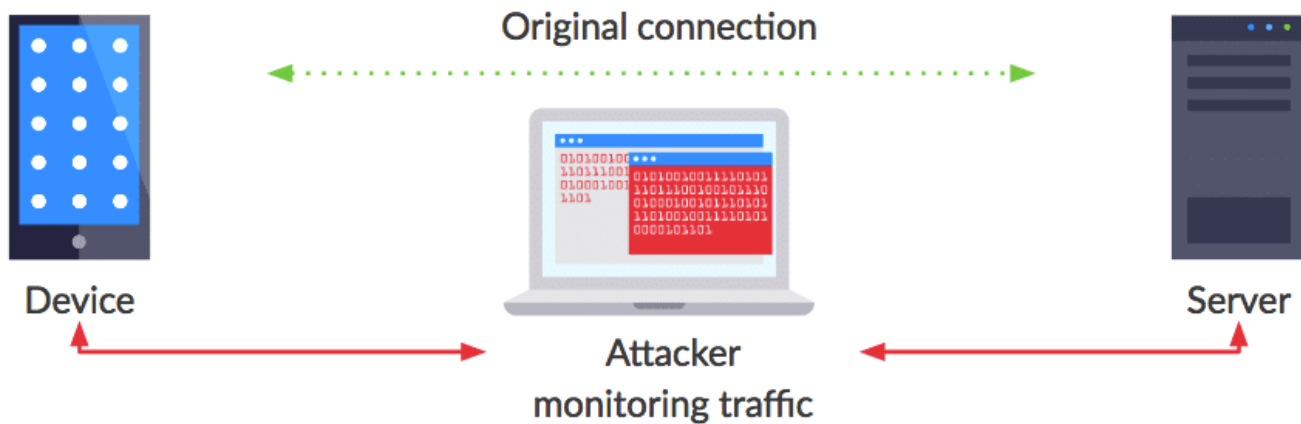
Password

☐ Remember me for two weeks [Forgot your password?](#)

Sign in

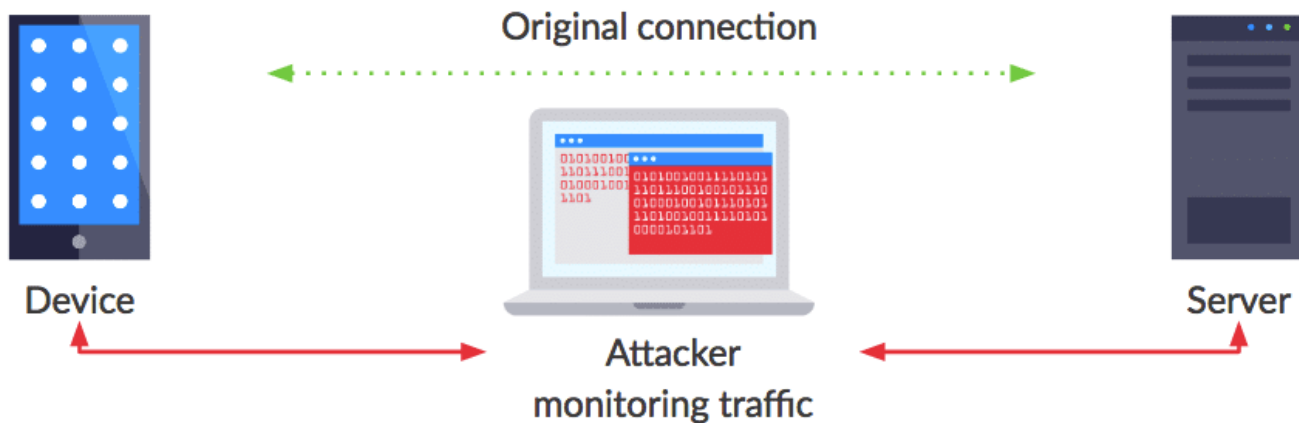


Intercept & Modify Request





Intercept & Modify Request



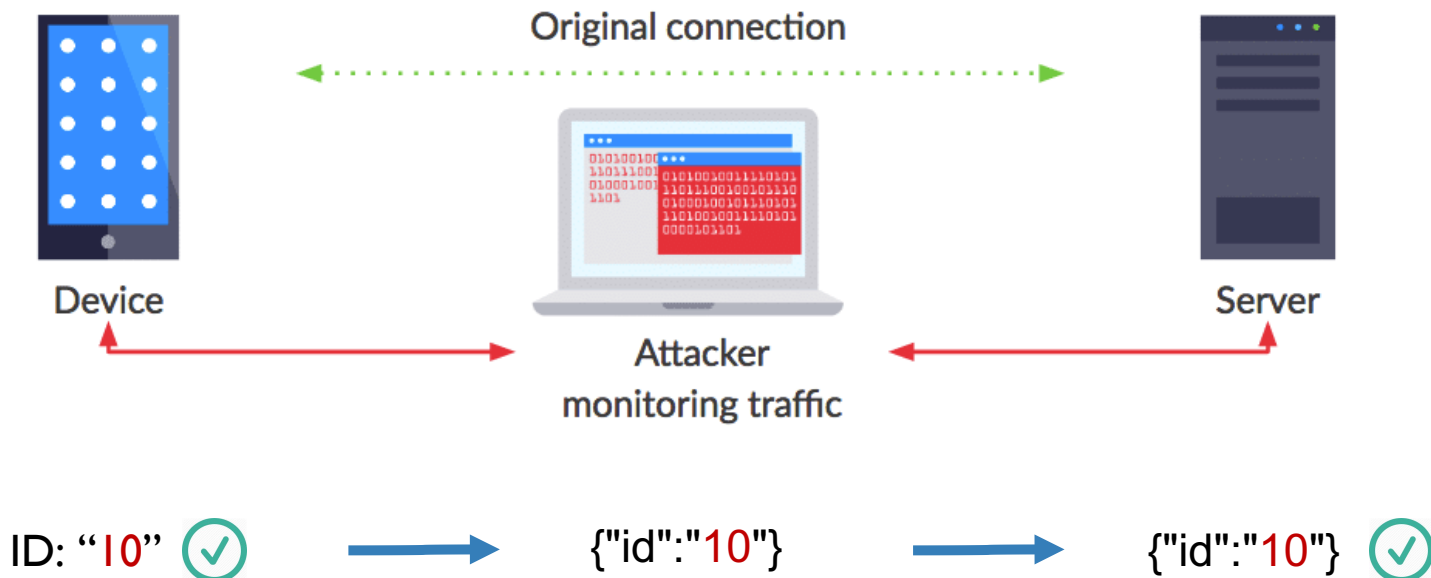
ID: "test <>" ❌

ID: "10" ✅

"ID must be in numeric"

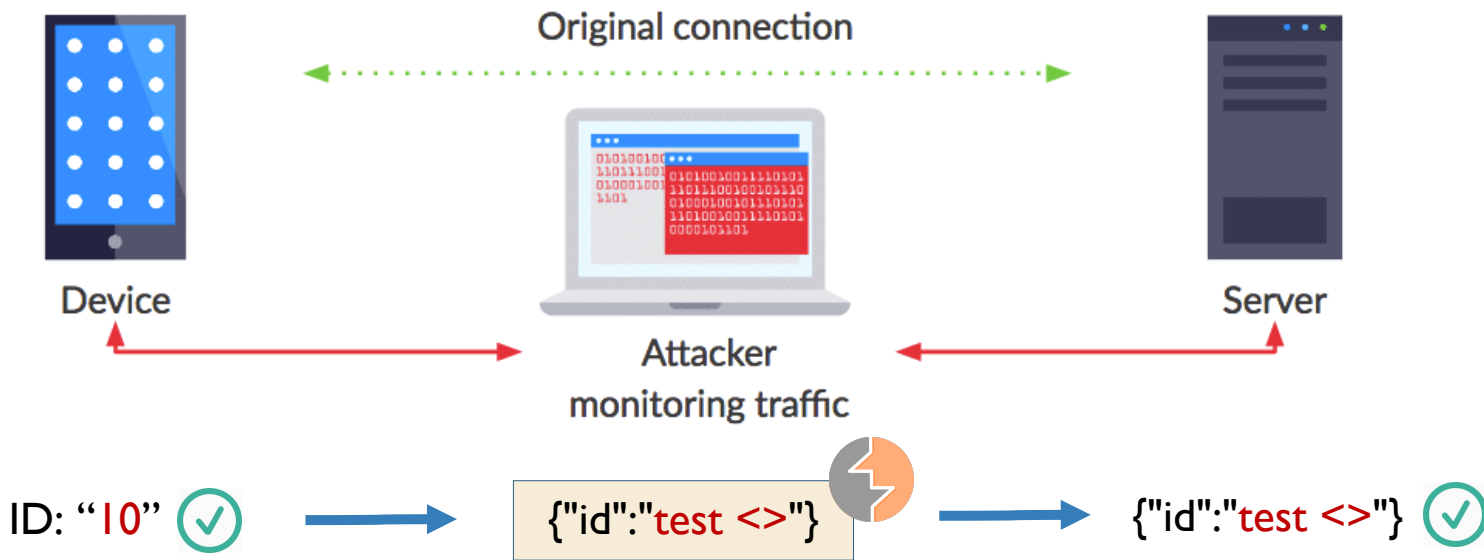


Intercept & Modify Request





Intercept & Modify Request





Intercept & Modify Request



mozilla
Firefox®



BURPSUITE



Intercept & Modify Request

Message Header

```
POST /api/vote HTTP/1.1
Host: hackyourselffirst.troyhunt.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:58.0) Gecko/20100101
Firefox/58.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://hackyourselffirst.troyhunt.com/Supercar/1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 34
Cookie: _ga=GA1.2.142313643.1527228892; ASP.NET_SessionId=ldxyepbdcljhgze45klvolnv;
VisitStart=6/3/2018 2:02:25 PM;
ARRAffinity=7dc50bf6149e01f9c7b990a468d5e06ac4e4699c1777460d3f2787ac530c2dd6;
_gid=GA1.2.1135597164.1528034547;
AuthCookie=B01664A991CA8121A961824687B3540E5BBC61514B6D0170CE1F590C8D788A59A00DCA00E
87B89376E06E9F0C67AEFE67EF64AA3DAB898383080BFAD9445440ED3445CCAF7B73048833648373785D
26EFC6C1B90949A2446535D8DF99E99DDB4221D4CA5ACC6C8667CC4A5A1E33BE31590AB362E82BA6A72E
4D6708CB09A347C; _gat=1
Connection: close
```

A blank line

```
userId=68&supercarId=1&comments=sa
```

Request Body



Intercept & Modify Request

Response Header

Response

Raw

Headers

Hex

```
HTTP/1.1 201 Created
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Server: Microsoft-IIS/10.0
X-XSS-Protection: 0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Sun, 03 Jun 2018 14:10:31 GMT
Connection: close
Content-Length: 0
```



Security Test Report

- Title:
- Details:
- Severity:
- Steps:
- Request:
- Response:
- Recommended:
- Screenshot:



Q/A!

W: www.sangbui.com

T: @sangsecurity

E: sangbuicom@gmail.com