Security Testing Course

W: www.sangbui.com
T: @sangsecurity
E: sangbuicom@gmail.com

OWASP
Open Web Application Security Project

Agenda

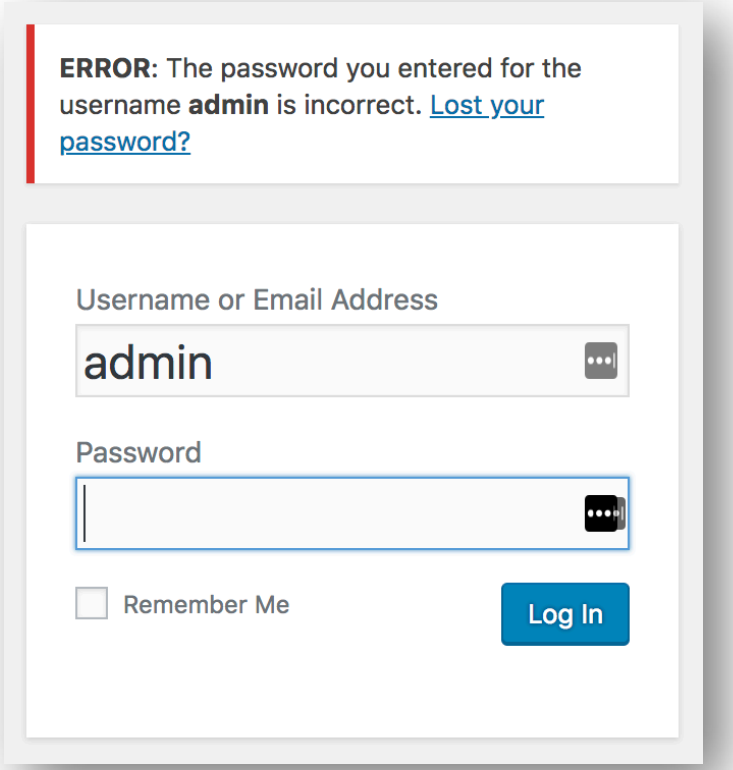
- Introducing
- Security Mindset
- Intercept & Modify Request
- Hands on Labs : Bypass the client side validation
- Security Test Report

Security Mindset

Security Bug (Defect)

Security Mindset

~~Security Bug (Defect)~~



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

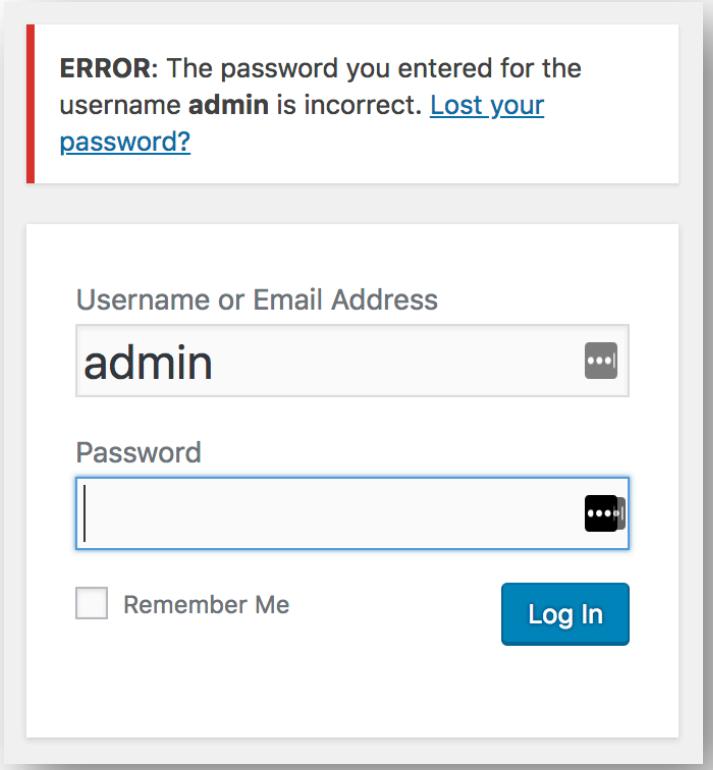
Even it is not a bug, but it still a risk

Risk = likelihood x impact

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

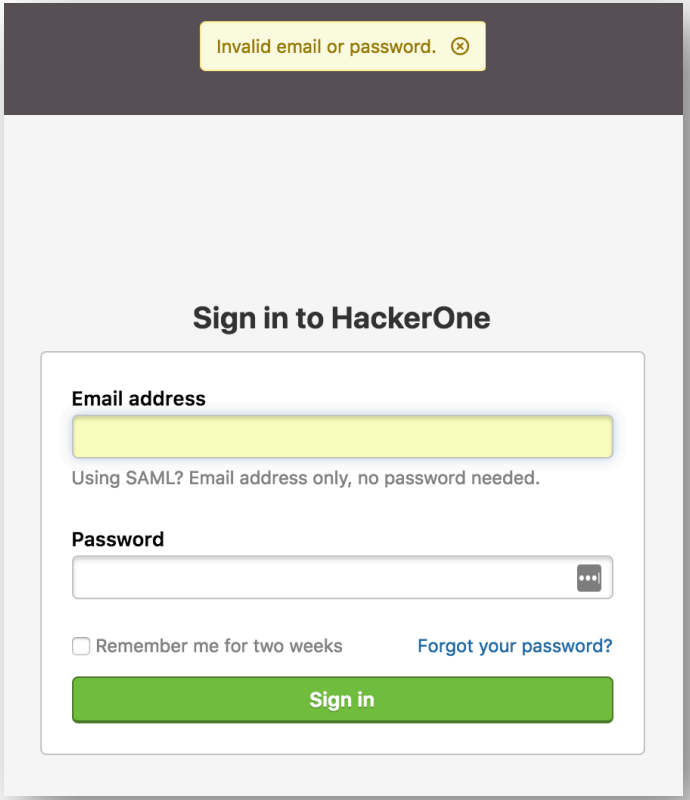
Security Mindset

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

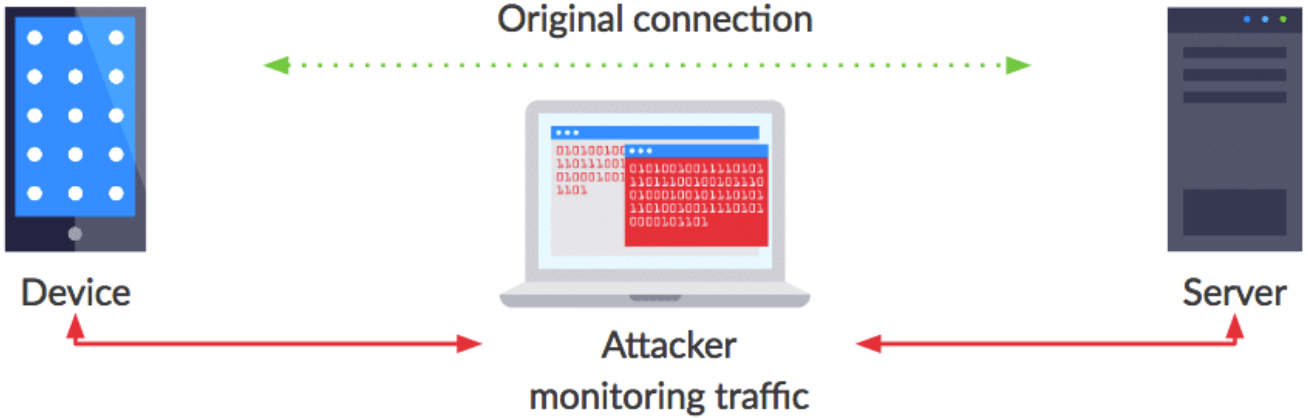


Security Mindset

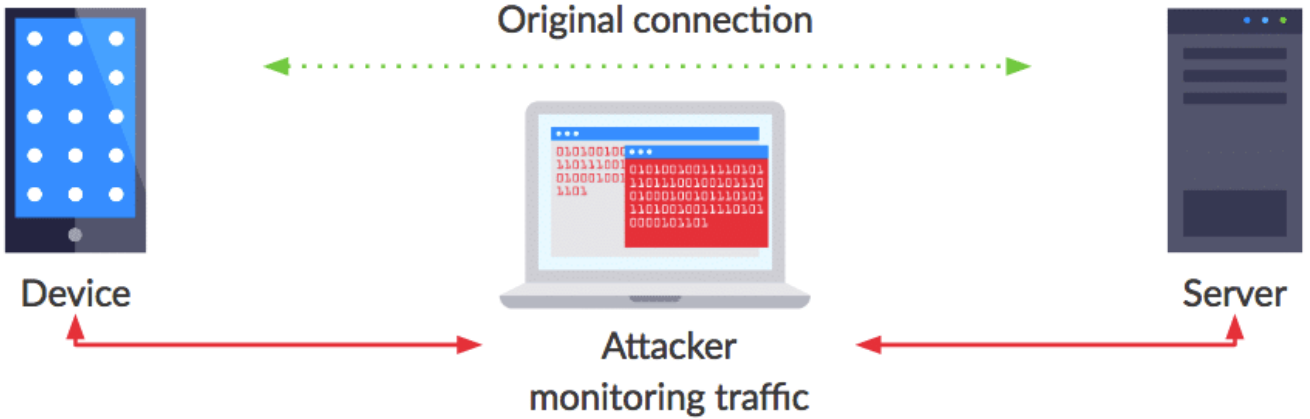
An application should respond with a *generic error message* regardless of whether the user ID or password was incorrect.



Intercept & Modify Request



Intercept & Modify Request

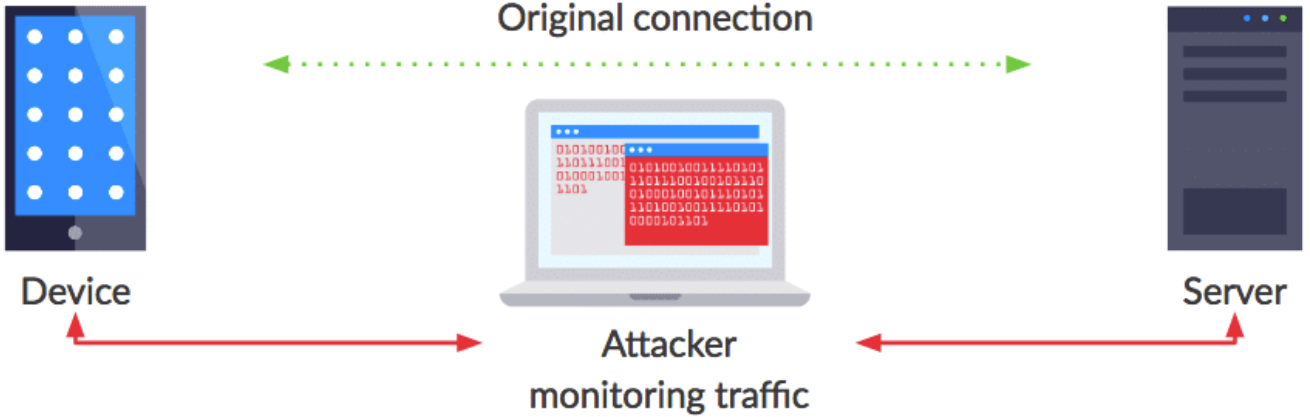


ID: “test <>”

ID: “10”

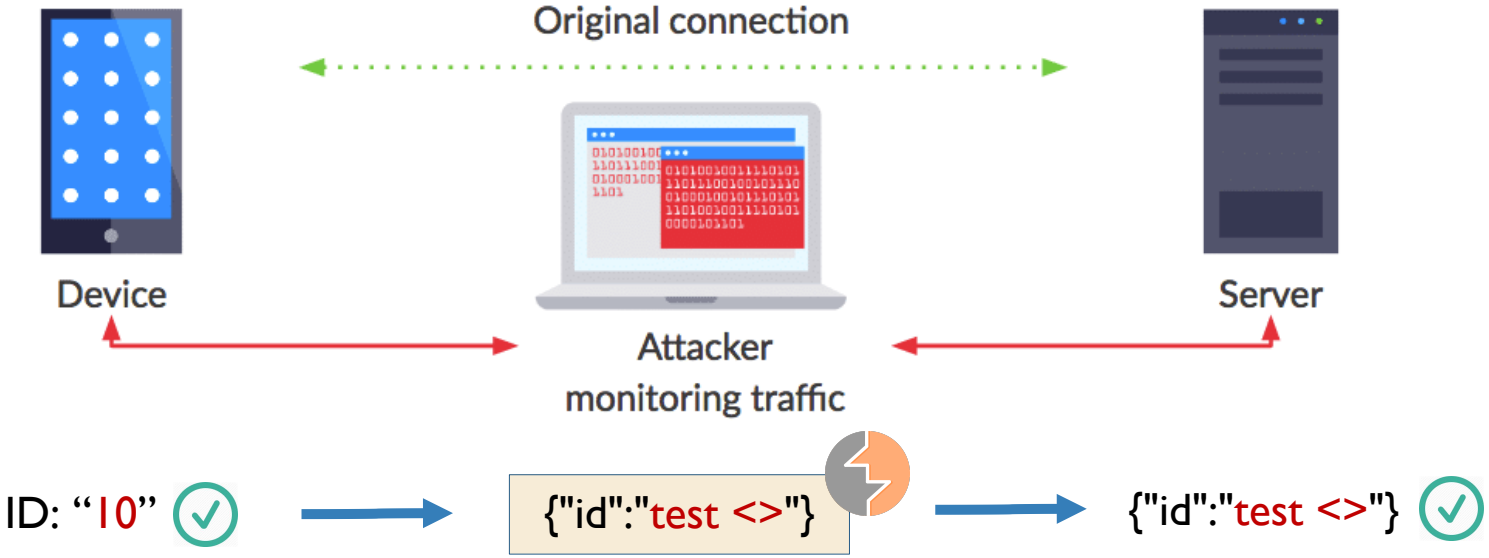
“ID must be in numeric”

Intercept & Modify Request



ID: “10” → {"id":"10"} → {"id":"10"}

Intercept & Modify Request



Intercept & Modify Request

Intercept & Modify Request

Message Header

A blank line

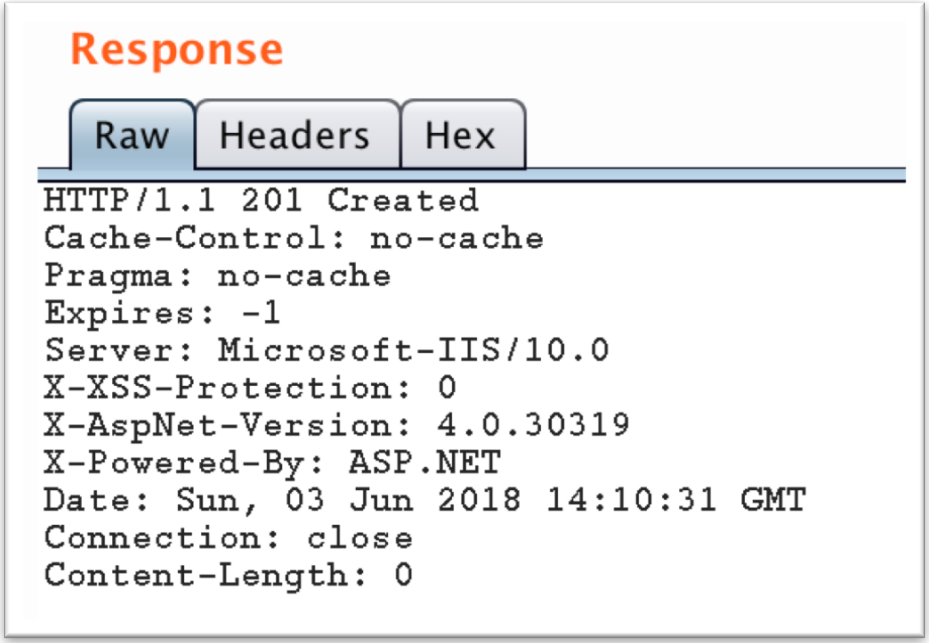
```
POST /api/vote HTTP/1.1
Host: hackyourselffirst.troyhunt.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:58.0) Gecko/20100101
Firefox/58.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://hackyourselffirst.troyhunt.com/Supercar/1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 34
Cookie: _ga=GA1.2.142313643.1527228892; ASP.NET_SessionId=ldxyepbdc1jhgze45k1volnv;
VisitStart=6/3/2018 2:02:25 PM;
ARRAffinity=7dc50bf6149e01f9c7b990a468d5e06ac4e4699c1777460d3f2787ac530c2dd6;
_gid=GA1.2.1135597164.1528034547;
AuthCookie=B01664A991CA8121A961824687B3540E5BBC61514B6D0170CE1F590C8D788A59A00DCA00E
87B89376E06E9F0C67AEFE67EF64AA3DAB898383080BFAD9445440ED3445CCAF7B73048833648373785D
26EFC6C1B90949A2446535D8DF99E99DDB4221D4CA5ACC6C8667CC4A5A1E33BE31590AB362E82BA6A72E
4D6708CB09A347C; _gat=1
Connection: close

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

Request Body

Intercept & Modify Request

Response Header



Security Test Report

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

Q/A!

W: www.sangbui.com

T: @sangsecurity

E: sangbuicom@gmail.com