



# OWASP

Open Web Application  
Security Project





# OWASP TOP 10 이란?

2004년 부터 현재까지 3~4년에 한번씩

주로 웹에 관한 취약점 중에서 빈도가 많이 발생하고,  
보안상 위협을 크게 줄 수 있는 것들을 10가지 선정하여

Top 10 으로 발표하고있는 보안프로젝트

## OWASP TOP 10

A1 - Injection	A6 – Security Misconfigurations
A2 – Broken Authentication	A7 – Cross Site Scripting (XSS)
A3 – Sensitive Data Exposure	A8 – Insecure Deserialization
A4 – XML External Entities (XXE)	A9 – Using Components with Known Vulnerabilities
A5 – Broken Access Control	A10 – Insufficient Logging and Monitoring

## OWASP TOP 10

A1 - Injection	A6 – Security Misconfigurations
A2 – Broken Authentication	A7 – Cross Site Scripting (XSS)
A3 – Sensitive Data Exposure	A8 – Insecure Deserialization
A4 – XML External Entities (XXE)	A9 – Using Components with Known Vulnerabilities
A5 – Broken Access Control	A10 – Insufficient Logging and Monitoring



# Broken Authentication

- “admin/admin”과 같은 약한 암호, 잘 알려진 암호를 허용
  - 다중 인증이 없음
  - 세션 ID가 URL에 노출
- 세션 ID를 무효화 시키지 않음
  - ...



# Broken Authentication

## 시나리오

#1. 잘 알려진 암호 목록을 이용하거나,  
무차별 대입 공격(브루트 포스)을 통해 계정을 알아낼 수 있다.

#2. 세션에 대한 적절한 만료 시간을 정해 놓지 않는다면,  
'로그아웃'을 선택하지 않고 단순히 브라우저 탭을 닫고 나갈 경우,  
다음 사용자가 이용할 때 여전히 인증되어 있어 이전사용자의 권한을 가질 수 있다.

# ...



## Broken Authentication – Password Attacks

✓ Broken Auth. - Password Attacks ✓

Enter your credentials (*bee/bug*).

Login:

Password:

rodiu



## Broken Authentication – Password Attacks

#

친구와 pc방에 같이 있는 상황

친구의 롤 아이디는 알고 있으며,

비밀번호를 입력할 때 슬쩍 봤더니

3글자이며, 영문으로 구성!!



## Broken Authentication – Password Attacks

The screenshot displays a web application interface on the left and the Burp Suite tool on the right. The web application has a 'Change Password' header and a login form with fields for 'Login' (containing 'bee') and 'Password' (containing 'bug'), and a 'Login' button. A green message 'Successful login!' is visible below the form. The Burp Suite window, titled 'Burp Suite Community Edition v2020.11.2 - Temporary Project', shows the 'Proxy' tab with 'Intercept' selected. A request to 'http://192.168.35.27:80' is being intercepted. The raw request data is shown in the 'Raw' tab, with the following details:

- 1 POST /bWAPP/ba\_pwd\_attacks\_1.php HTTP/1.1
- 2 Host: 192.168.35.27
- 3 Content-Length: 34
- 4 Cache-Control: max-age=0
- 5 Upgrade-Insecure-Requests: 1
- 6 Origin: http://192.168.35.27
- 7 Content-Type: application/x-www-form-urlencoded
- 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.
- 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image;q=0.9
- 10 Referer: http://192.168.35.27/bWAPP/ba\_pwd\_attacks\_1.php
- 11 Accept-Encoding: gzip, deflate
- 12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
- 13 Cookie: PHPSESSID=133fc673a7fb7fa7ed76d381281640e1; security\_level=0
- 14 Connection: close
- 15
- 16 login=bee&password=bug&form=submit

The raw request data is highlighted with a red box, showing the payload: `login=bee&password=bug&form=submit`.



## Broken Authentication – Password Attacks

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Compare

Intercept HTTP history WebSockets history Options

Request to http://192.168.35.27:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Wn Actions

```
1 POST /bWAPP/ba_pwd_attacks_1.php HTTP/1.1
2 Host: 192.168.35.27
3 Content-Length: 34
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.35.27
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win
9 Accept:
  text/html,application/xhtml+xml,application/x
  q=0.9
10 Referer: http://192.168.35.27/bWAPP/ba_pwd_at
11 Accept-Encoding: gzip, deflate
12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,e
13 Cookie: PHPSESSID=133fc673a7fb7fa7ed76d381281
14 Connection: close
15
16 login=bee&password=bug&form=submit
```

- Scan
- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser >
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding

Dashboard Target Proxy Intruder Repeater

1 x 2 x -

Target Positions Payloads Options

? Attack Target

Configure the details of the target for the attack.

Host: 192.168.35.27

Port: 80

☐ Use HTTPS



## Broken Authentication – Password Attacks

Buttons for interaction:

- Add \$
- Clear \$
- Auto \$
- Refresh

Attack type: Sniper

```
1 POST /bWAPP/ba_pwd_attacks_1.php HTTP/1.1
2 Host: 192.168.35.27
3 Content-Length: 34
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.35.27
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
10 Referer: http://192.168.35.27/bWAPP/ba_pwd_attacks_1.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: PHPSESSID=$133fc673a7fb7fa7ed76d381c81640e1$;
14 Connection: close
15
16 login=$bee$&password=$bug$&form=$submit$
```

login=bee&password=\$bug\$&form=submit

Attack type: Sniper

```
1 POST /bWAPP/ba_pwd_attacks_1.php HTTP/1.1
2 Host: 192.168.35.27
3 Content-Length: 34
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.35.27
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
10 Referer: http://192.168.35.27/bWAPP/ba_pwd_attacks_1.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: PHPSESSID=133fc673a7fb7fa7ed76d381c81640e1;
14 Connection: close
15
16 login=bee&password=bug&form=submit
```



## Broken Authentication – Password Attacks

Target

Positions

Payloads

Options

?

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on how they are customized in different ways.

Payload set:

1

▼

Payload count:

17,576

Payload type:

Brute forcer

▼

Request count:

17,576

?

**Payload Options [Brute forcer]**

This payload type generates payloads of specified lengths that contain all permutations of the specified character set.

Character set:

abcdefghijklmnopqrstuvwxyz

Min length:

3

Max length:

3

Target

Positions

Payloads

Options

?

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on how they are customized in different ways.

Payload set:

1

▼

Payload count:

27

Payload type:

Brute forcer

▼

Request count:

27

?

**Payload Options [Brute forcer]**

This payload type generates payloads of specified lengths that contain all permutations of the specified character set.

Character set:

bgu

Min length:

3

Max length:

3



## Broken Authentication – CAPTCHA Bypassing

### / Broken Auth.

Enter your credentials (*bee/bug*).

Login:

Password:

Login

Successful login!

### / Broken Auth. - Password Attacks /

Enter your credentials (*bee/bug*).

Login:

Password:

Login

Invalid credentials! Did you forgot your password?



## Broken Authentication – Password Attacks

The screenshot shows the 'Options' tab in Burp Suite's 'Grep - Match' configuration window. The window has tabs for 'Target', 'Positions', 'Payloads', and 'Options'. The 'Options' tab is active. Below the tabs, there is a help icon and the title 'Grep - Match'. A refresh icon is followed by the text: 'These settings can be used to flag result items containing specified expressions.' A checked checkbox is labeled 'Flag result items with responses matching these expressions:'. To the left of a large text input area are four buttons: 'Paste', 'Load ...', 'Remove', and 'Clear'. The text input area contains the string 'Invalid credentials! Did you forgot your password?'. To the right of the input area is a red arrow pointing right. Below the input area is an 'Add' button and a preview box containing the text 'alid credentials! Did you forgot your password?'. At the bottom, the 'Match type' section has two radio buttons: 'Simple string' (selected) and 'Regex'. There are two checkboxes: 'Case sensitive match' (unchecked) and 'Exclude HTTP headers' (checked).

Target Positions Payloads Options

? **Grep - Match**

These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste Load ... Remove Clear

Invalid credentials! Did you forgot your password?

Add alid credentials! Did you forgot your password?

Match type: ☒ Simple string ☐ Regex

☐ Case sensitive match ☒ Exclude HTTP headers



## Broken Authentication – Password Attacks

Attack 4

Back Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request ^	Payload	Status	Error	Timeout	Length	Invalid c...	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	13898	<input type="checkbox"/>	
1	bbb	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
2	gbb	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
3	ubb	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
4	bgb	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
5	ggb	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
6	ugb	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
7	bub	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
8	gub	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
9	uub	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
10	bbg	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
11	gbg	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
12	ubg	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
13	bgg	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
14	ggg	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
15	ugg	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
16	bug	200	<input type="checkbox"/>	<input type="checkbox"/>	13898	<input type="checkbox"/>	
17	gug	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
18	uug	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
19	bbu	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
20	gbu	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
21	ubu	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
22	bg u	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
23	gg u	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
24	ug u	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
25	buu	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
26	guu	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	
27	uuu	200	<input type="checkbox"/>	<input type="checkbox"/>	13929	<input checked="" type="checkbox"/>	

Finished



# How to prevent Password Attacks

- 약한 비밀번호 검사
- 다중 인증 구현
- 로그인 실패에 대한 로그를 남기고,  
무차별 공격 등이 탐지됐을 때, 관리자에게 알림
- Salt 이용
- ...



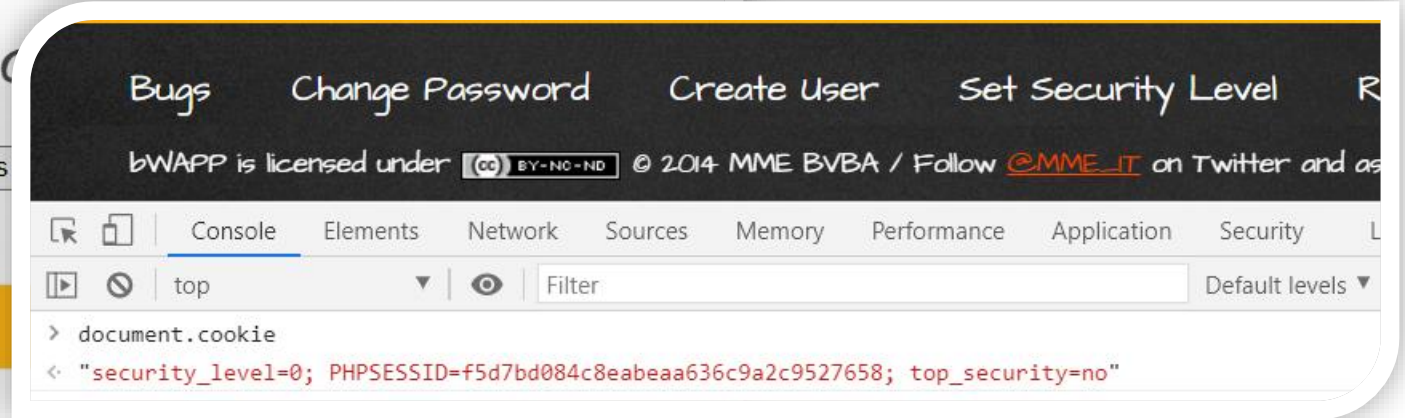
## ▼ Session management – Cookies (HTTPOnly)

### / Session Mgmt. - Co

Click the button to see your current cookies: [Cookies](#)

Click [here](#) to see your cookies with JavaScript.

Name	Value
security_level	0
PHPSESSID	f5d7bd084c8eabeaa636c9a2c9527658
top_security	no



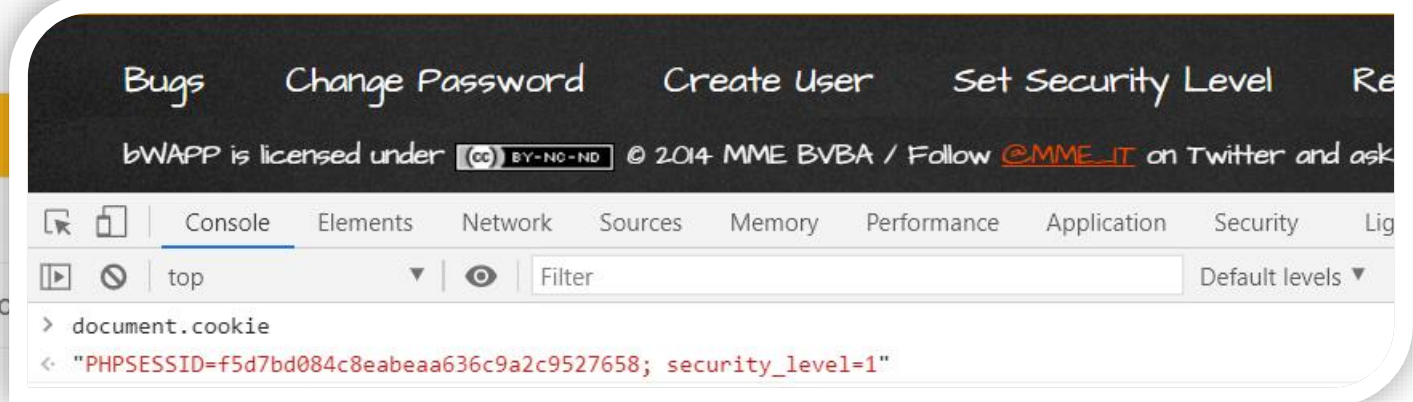
## Session management – Cookies (HTTPOnly)

### / Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: [Cookies](#)

Click [here](#) to see your cookies with JavaScript.

Name	Value
security_level	0
PHPSESSID	f5d7bd084c8eabeaa636c9a2c9527658
top_security	no



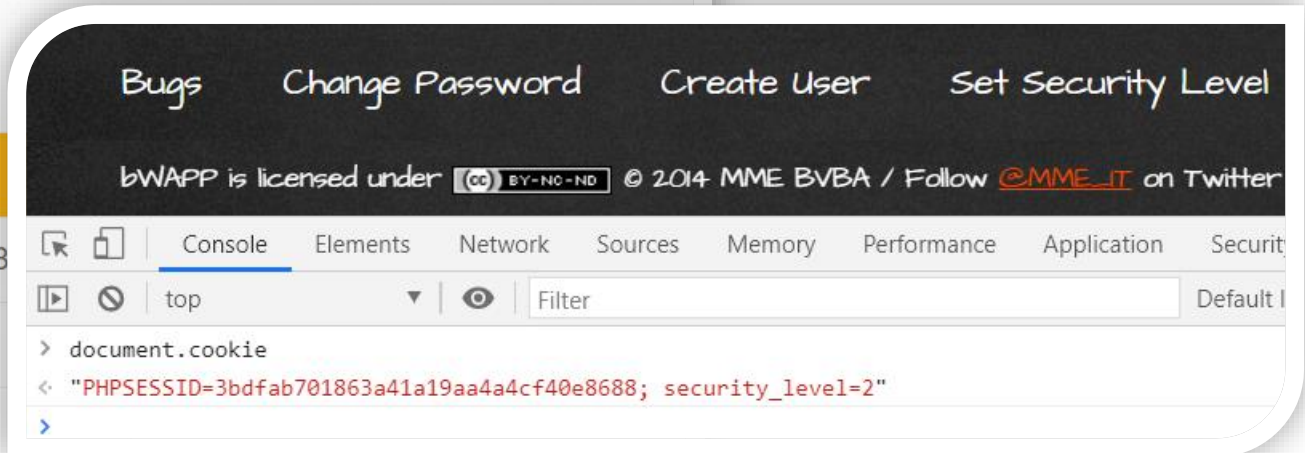
## Session management – Cookies (HTTPOnly)

### / Session Mgmt. - Cookies (HTTPOnly) /

Click the button to see your current cookies: Cookies

Click **here** to see your cookies with JavaScript.

Name	Value
PHPSESSID	3bdfab701863a41a19aa4a4cf40e868
security_level	2
top_security	yes





## Session management – Cookies (HTTPOnly)

```
if (isset($_COOKIE["security_level"]))
```

setcookie (쿠키명, 쿠키값, 만료시간, 경로, 도메인, secure, httponly);

```
case "0" :
```

```
// The cookie will be available within the entire domain
setcookie("top_security", "no", time()+3600, "/", "", false, false);
break;
```

```
case "1" :
```

```
// The cookie will be available within the entire domain
// Sets the Http Only flag
setcookie("top_security", "maybe", time()+3600, "/", "", false, true);
break;
```

```
case "2" :
```

```
// The cookie will be available within the entire domain
// The cookie expires at end of the session
// Sets the Http Only flag
setcookie("top_security", "yes", time()+300, "/", "", false, true);
break;
```

```
default :
```

```
// The cookie will be available within the entire domain
setcookie("top_security", "no", time()+3600, "/", "", false, false);
break;
```

```
}
```



## Session management – Cookies (HTTPOnly)

The screenshot shows a web browser's developer tools interface. At the top, it says "Request to http://192.168.35.27:80". Below this are several buttons: "Forward", "Drop", "Intercept is on", "Action", and "Open Browser". Underneath these buttons are tabs for "Pretty", "Raw", "Wn", and "Actions". The "Raw" tab is selected, displaying the raw HTTP request. The request is a GET request to the path "/bWAPP/smgmt\_cookies\_httponly.php" with HTTP version "1.1". The headers include "Host: 192.168.35.27", "Cache-Control: max-age=0", "Upgrade-Insecure-Requests: 1", "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)", "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.9", "Referer: http://192.168.35.27/bWAPP/smgmt\_cookies\_httponly.php", "Accept-Encoding: gzip, deflate", and "Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7". The Cookie header is "PHPSESSID=3bdfab701863a41a19aa4a4cf40e8688; security\_level=2; top\_security=yes". The request ends with "Connection: close".

```
1 GET /bWAPP/smgmt_cookies_httponly.php HTTP/1.1
2 Host: 192.168.35.27
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.9
7 Referer: http://192.168.35.27/bWAPP/smgmt_cookies_httponly.php
8 Accept-Encoding: gzip, deflate
9 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
10 Cookie: PHPSESSID=3bdfab701863a41a19aa4a4cf40e8688; security_level=2; top_security=yes
11 Connection: close
12
13
```



## Session management – Cookies (Secure)

### / Session Mgmt. - Cookies (Secure) /

Click the button to see your current cookies: [Cookies](#)

Browse to another page to see if the cookies are protected over a non-SSL channel.

Name	Value
PHPSESSID	3bdfab701863a41a19aa4a4cf40e8688
security_level	0
top_security	no



## Session management – Cookies (Secure)

### / Session Mgmt. - Cookies (Secure) /

Click the button to see your current cookies: [Cookies](#)

Browse to another page to see if the cookies are protected over a non-SSL channel.

Name	Value
PHPSESSID	3bdfab701863a41a19aa4a4cf40e8688
security_level	0
top_security	no





## Session management – Cookies (Secure)

### / Session Mgmt. - Cookies (Secure) /

Click the button to see your current cookies: [Cookies](#)

This page must be accessed over a SSL channel to fully function!

Browse to another page to see if the cookies are protected over a non-SSL channel.

Name	Value
PHPSESSID	3bdfab701863a41a19aa4a4cf40e8688
security_level	2





## Session management – Cookies (Secure)

### / Session Mgmt. - Cookies (Secure) /

Click the button to see your current cookies: [Cookies](#)

This page must be accessed over a SSL channel to fully function!

Browse to another page to see if the cookies are protected over a non-SSL channel.

Name	Value
PHPSESSID	3bdfab701863a41a19aa4a4cf40e8688
security_level	2
top_security	yes



## Session management – Cookies (Secure)

setcookie (쿠키명, 쿠키값, 만료시간, 경로, 도메인, secure, httponly);

```
if($_COOKIE["security_level"])

case "0" :

    $message.= "<p>Browse to another page to see if the cookies are protected over a non-SSL channel.</p>";

    // The cookie will be available within the entire domain
    // Sets the Http Only flag
    setcookie("top_security", "no", time()+3600, "/", "", false, true);
    break;

case "1" :

    $message = "<p>This page must be accessed over a SSL channel to fully function!<br />";
    $message.= "Browse to another page to see if the cookies are protected over a non-SSL channel.</p>";

    // The cookie will be available within the entire domain
    // Sets the Http Only flag and the Secure flag
    setcookie("top_security", "maybe", time()+3600, "/", "", true, true);
    break;

case "2" :

    $message = "<p>This page must be accessed over a SSL channel to fully function!<br />";
    $message.= "Browse to another page to see if the cookies are protected over a non-SSL channel.</p>";

    // The cookie will be available within the entire domain
    // The cookie expires at end of the session
    // Sets the Http Only flag and the Secure flag
    setcookie("top_security", "yes", time()+300, "/", "", true, true);
    break;

default :

    $message.= "<p>Browse to another page to see if the cookies are protected over a non-SSL channel</p>";

    // The cookie will be available within the entire domain
    // Sets the Http Only flag
    setcookie("top_security", "no", time()+3600, "/", "", false, true);
    break;;
```

## OWASP TOP 10

A1 - Injection	A6 – Security Misconfigurations
A2 – Broken Authentication	A7 – Cross Site Scripting (XSS)
A3 – Sensitive Data Exposure	A8 – Insecure Deserialization
A4 – XML External Entities (XXE)	A9 – Using Components with Known Vulnerabilities
A5 – Broken Access Control	A10 – Insufficient Logging and Monitoring