禪

[redacted]

[redacted]

[redacted]

[redacted]

NextGenEditor [redacted] inlineediting pagebuilder [redacted] 40 [redacted]
[redacted] SQL [redacted]
http://localhost/[PATH]/index.php?option=com_nge&view=config&plname=[SQL

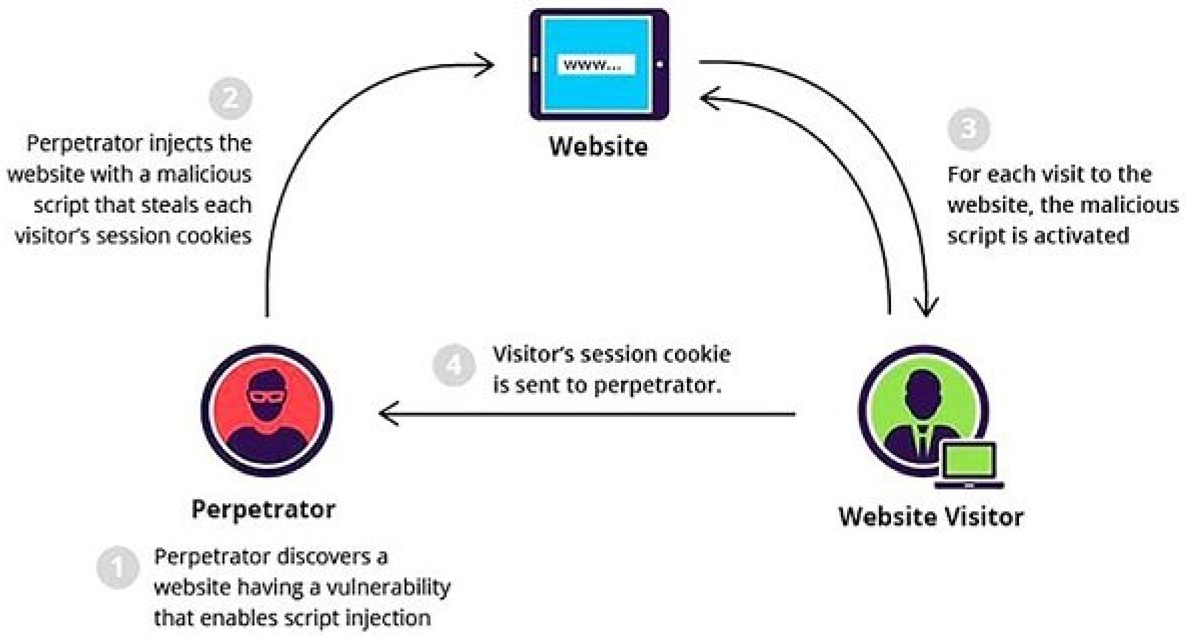
[illegible] SQL [illegible]

[illegible] SOCKS [illegible] Linux.ProxyM [illegible] SOCKS [illegible] MIPS، MIPSEL، PowerPC، x86، Superh، Motorola 68000، SPARC [illegible] (set-top boxes) [illegible] 400 [illegible]

[illegible] DocuSign [illegible] Linux.ProxyM [illegible] SQL [illegible] 40 [illegible] 7 [illegible] 20 [illegible] SQL [illegible] (SQL) [illegible]

[illegible]

[illegible] Cross Site Scripting [illegible] XSS [illegible] (1 [illegible])



[illegible] SQL injection [illegible]

[illegible] ([illegible]) [illegible] SQL [illegible] (Dll Injection) [illegible] SQL [illegible] Imperva [illegible] SQL [illegible] 2007 [illegible] 2010 [illegible] 10 [illegible].

[illegible]Classic SQLIA

[illegible]Inference SQL injection

Interacting with SQL injectio
Database management system-specific SQLIA
Compounded SQLIA
SQL injection + insufficient authentication
SQL injection + DDoS attacks
SQL injection + DNS hijacking
SQL injection + XSS
SQL injection + Filter bypass + Havij + Backtrack R6

[illegible]

[illegible]
;" "'=Select * From Persons Where username
[illegible]:Select
[illegible].
[illegible]:From
[illegible].
[illegible]:Where
[illegible].
[illegible]:Other statements
[illegible].
[illegible] SQL Injection [illegible].
;var Shipcity
;("ShipCity = Request.form ("ShipCity
;"'" + var sql = "select * from OrdersTable where ShipCity = '" + ShipCity
[illegible]:
'SELECT * FROM OrdersTable WHERE ShipCity = 'Redmond
[illegible]:
--Redmond'; drop table OrdersTable
[illegible]:
'--SELECT * FROM OrdersTable WHERE ShipCity = 'Redmond';drop table OrdersTable
[illegible] ShipCity [illegible] OrdersTable [illegible] Sql Server [illegible]

[illegible] OrdersTable [illegible] Redmond [illegible] SQL [illegible]

[illegible]

[illegible]:

- [illegible].
- [illegible].
- DROP TABLE [illegible] 10 [illegible].
- [illegible].
- [illegible] (Buffer Overrun) [illegible].
- [illegible].
- XML [illegible] Buffer Overrun [illegible].
- TSQL [illegible].
- [illegible].
- [illegible].
- [illegible].
- [illegible].
- [illegible]:

AUX, CLOCK$, COM1 through COM8, CON, CONFIG$, LPT1,LPT8, NUL, and PRN

- [illegible].
- [illegible] _ xp /*....*/ -- , ; [illegible].
- [illegible] SQL [illegible] Parameter. [illegible] SQL [illegible] SQL [illegible]:

```
;(SqlDataAdapter myCommand = new SqlDataAdapter(“AuthorLogin”, conn
;myCommand.SelectCommand.CommandType = CommandType.StoredProcedure
SqlParameter parm = myCommand.SelectCommand.Parameters.Add(“@au_id”,
;( SqlDbType.VarChar, 11
;parm.Value = Login.Text
```

au_id@ [illegible] au-id@ [illegible].

- XSS [illegible].

[illegible] (Content Security Policy) [illegible]. [illegible]

:[illegible]

[illegible]

:[illegible]

technet.microsoft

securityweek

packetstormsecurity

owasp

imperva

:[illegible]

[illegible]

:[illegible]

08:30 - 10/12/1397

:[illegible]

SQL injection - [illegible]

[illegible]

[illegible]: https://www.shabakeh-mag.com/security/14672/%D8%AD%D9%85%D9%84%D9%87-%D8%AA%D8%B2%D8%B1%DB%8C%D9%82-%DA%A9%D8%AF-%D8%B1%D8%A7-%D8%A8%D8%B4%D9%86%D8%A7%D8%B3%DB%8C%D8%AF